

Pocket No. 217201US8/btm



2131  
#3  
KWS  
4-11-02

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Shoji FUKUTOMI

GAU: 2131

SERIAL NO: 10/020,227

EXAMINER:

FILED: December 18, 2001

FOR: MULTICAST AUTHENTICATION METHOD, MULTICAST AUTHENTICATION SERVER, NETWORK INTERCONNECTION APPARATUS AND MULTICAST AUTHENTICATION SYSTEM

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS  
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number [US App No], filed [US App Dt], is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY

JAPAN

APPLICATION NUMBER

2001-209929

MONTH/DAY/YEAR

July 10, 2001

RECEIVED

FEB 14 2002

Technology Center 2100

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and  
(B) Application Serial No.(s)
  - ☐ are submitted herewith
  - ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

Bradley D. Lytle  
Registration No. 40,073

Joseph A. Scafetta, Jr.  
Registration No. 26,803



22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 10/98)



10/020,227  
PLEA 01032-VS

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office

出 願 年 月 日

Date of Application:

2001年 7月10日

出 願 番 号

Application Number:

特願2001-209929

[ST.10/C]:

[JP2001-209929]

出 願 人

Applicant(s):

古河電気工業株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

RECEIVED

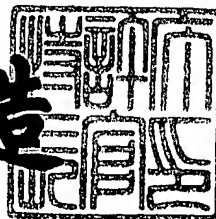
FEB 14 2002

Technology Center 2100

2002年 1月22日

特許庁長官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2002-3000382

【書類名】 特許願

【整理番号】 A10263

【提出日】 平成13年 7月10日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/56

【発明者】

    【住所又は居所】 東京都千代田区丸の内2丁目6番1号 古河電気工業株式会社内

    【氏名】 福富 昌司

【特許出願人】

    【識別番号】 000005290

    【氏名又は名称】 古河電気工業株式会社

【代理人】

    【識別番号】 100089118

    【弁理士】

    【氏名又は名称】 酒井 宏明

【手数料の表示】

    【予納台帳番号】 036711

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 0103421

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 マルチキャスト認証方法、その認証サーバ、ネットワーク間接続装置およびマルチキャスト認証システム

【特許請求の範囲】

【請求項 1】 複数の受信者ホストと送信者ホストのネットワーク網とがネットワーク間接続装置を介して接続されるとともに、前記ネットワーク網内の認証サーバによって前記送信者ホストのマルチキャストグループへの参加を認証するマルチキャスト認証方法において、

前記受信者ホストからの前記送信者ホストのマルチキャストグループへの参加申し込みに応じて、当該受信者ホストのアドレスを前記認証サーバに登録する登録工程と、

前記受信者ホストからの参加要求のメッセージに対し、前記認証サーバの登録内容に基づいて受信者ホストの認証を行う認証工程とを含むことを特徴とするマルチキャスト認証方法。

【請求項 2】 複数の受信者ホストと送信者ホストのネットワーク網とがネットワーク間接続装置および中継装置を介して接続されるとともに、前記ネットワーク網内の認証サーバによって前記送信者ホストのマルチキャストグループへの参加を認証するマルチキャスト認証方法において、

前記受信者ホストから前記送信者ホストのマルチキャストグループへの参加申し込みに応じて、当該受信者ホストが接続されている前記中継装置のアドレスを前記認証サーバに登録する登録工程と、

前記受信者ホストからの参加要求のメッセージに対し、前記認証サーバの登録内容に基づいて前記中継装置の認証を行う認証工程とを含むことを特徴とするマルチキャスト認証方法。

【請求項 3】 前記マルチキャスト認証方法では、前記参加要求のメッセージに対して前記受信者ホストの認証がなされると、前記マルチキャストグループへの当該受信者ホストの参加を許可する許可工程をさらに含むことを特徴とする請求項 1 または 2 に記載のマルチキャスト認証方法。

【請求項 4】 前記登録工程では、前記受信者ホストまたは前記中継装置の

アドレスとともに、当該受信者ホストまたは当該中継装置が接続されている前記ネットワーク間接続装置のポートの情報を前記認証サーバに登録することを特徴とする請求項 1～3 の少なくとも一つに記載のマルチキャスト認証方法。

【請求項 5】 前記登録工程では、前記マルチキャストグループのグループアドレスをさらに前記認証サーバに登録し、

前記認証工程では、前記受信者ホストからの参加要求のメッセージに対し、前記認証サーバの登録内容に基づいて前記受信者ホストまたは前記中継装置と前記マルチキャストグループの認証を行うことを特徴とする請求項 1～4 に記載のマルチキャスト認証方法。

【請求項 6】 前記登録工程では、全ての前記マルチキャストグループへの参加の申し込みに応じて、前記受信者ホストまたは前記中継装置のアドレスを前記認証サーバに登録し、

前記許可工程では、前記参加要求のメッセージに対して前記受信者ホストの認証がなされると、全ての前記マルチキャストグループへの当該受信者ホストの参加を許可することを特徴とする請求項 1～5 に記載のマルチキャスト認証方法。

【請求項 7】 前記登録工程では、前記マルチキャストグループへの参加を許可する許可時間をさらに前記認証サーバに登録し、

前記許可工程では、参加要求のメッセージに対して前記受信者ホストの認証がなされると、前記許可時間内での前記マルチキャストグループへの当該受信者ホストの参加を許可することを特徴とする請求項 1～6 の少なくとも一つに記載のマルチキャスト認証方法。

【請求項 8】 前記登録工程では、前記受信者ホストまたは中継装置のアドレスと、前記マルチキャストグループのグループアドレスとの組を一つのユーザーネームとして登録し、

前記認証工程では、前記参加要求メッセージに含まれる送信元アドレスとグループアドレスを抽出し、当該送信元アドレスとグループアドレスの組を一つのユーザーネームとして、前記認証サーバの登録内容を検索して前記受信者ホストまたは中継装置の認証を行うことを特徴とする請求項 5～7 に記載のマルチキャスト認証方法。

【請求項 9】 前記許可工程では、前記許可時間は、前記マルチキャストグループごとに予め設定されており、前記参加申し込みの際に、前記受信者ホストによって指定された前記マルチキャストグループへの参加時間に基づいて、該受信者ホストに対する許可時間を設定して前記認証サーバに登録することを特徴とする請求項 7 に記載のマルチキャスト認証方法。

【請求項 10】 前記許可工程では、前記許可時間は、前記マルチキャストグループごとに予め設定されており、前記参加申し込みの際に、前記受信者ホストによって指定された前記マルチキャストグループに基づいて、前記許可時間を前記認証サーバに登録することを特徴とする請求項 7 に記載のマルチキャスト認証方法。

【請求項 11】 前記認証工程は、前記認証サーバが行い、認証結果とともに、前記受信者ホストがユーザ登録されている場合には、当該登録内容である許可時間の情報を前記ネットワーク間接続装置に送信し、

前記許可工程は、前記ネットワーク間接続装置が行い、受信した前記認証結果に基づいて参加の許可を判断するとともに、受信した前記許可時間内での前記マルチキャストグループへの前記受信者ホストの参加を許可することを特徴とする請求項 7, 9 および 10 の少なくとも一つに記載のマルチキャスト認証方法。

【請求項 12】 前記認証工程および許可工程は、前記ネットワーク間接続装置が行い、前記認証サーバは、前記参加申し込みの際に、指定された前記送信元アドレスとマルチキャストグループに対するユーザ登録内容を前記ネットワーク間接続装置に送信し、

該ネットワーク間接続装置は、当該登録内容に基づいて前記受信者ホストの認証を行って、前記認証結果に基づいて参加の許可を判断するとともに、前記許可時間内での前記マルチキャストアドレスグループへの参加を許可することを特徴とする請求項 7, 9 および 10 の少なくとも一つに記載のマルチキャスト認証方法。

【請求項 13】 前記認証工程では、前記許可時間にならないと認証の失敗と判断することを特徴とする請求項 7 ～ 12 の少なくとも一つに記載のマルチキャスト認証方法。

【請求項 1 4】 前記許可工程では、前記マルチキャストのユーザ登録を行い、前記認証工程で認証失敗と判断されると、該当するユーザ登録のエントリを削除することを特徴とする請求項 3，5～7 および 9～12 の少なくとも一つに記載のマルチキャスト認証方法。

【請求項 1 5】 前記マルチキャスト認証方法では、前記送信者ホストは、インターネットのサービス事業者であり、該サービス事業者が配信サーバによるコンテンツのストリーム配信サービスを行っており、前記許可工程では、前記許可時間内に前記配信サーバから配信されるコンテンツのストリームを、前記認可された受信者ホストへマルチキャストフォワーディングすることを特徴とする請求項 1～14 の少なくとも一つに記載のマルチキャスト認証方法。

【請求項 1 6】 前記マルチキャスト認証方法では、実行されたサービスに応じて課金する課金工程をさらに含むことを特徴とする請求項 1～15 の少なくとも一つに記載のマルチキャスト認証方法。

【請求項 1 7】 送信者ホストのネットワーク網内に設置される認証サーバにおいて、

前記送信者ホストのネットワーク網に接続される受信者ホストからの前記送信者ホストのマルチキャストグループへの参加申し込みに応じて、当該受信者ホストのアドレスを登録する登録手段を備えたことを特徴とする認証サーバ。

【請求項 1 8】 送信者ホストのネットワーク網内に設置される認証サーバにおいて、

中継装置を介して前記送信者ホストのネットワーク網に接続される受信者ホストからの前記送信者ホストのマルチキャストグループへの参加申し込みに応じて、当該中継装置のアドレスを登録する登録手段を備えたことを特徴とする認証サーバ。

【請求項 1 9】 前記認証サーバは、前記受信者ホストからの参加要求のメッセージに対し、前記登録手段の登録内容に基づいて参加の認証を行う認証手段と、

前記認証結果を送信する送信手段とをさらに備えたことを特徴とする請求項 17 または 18 に記載の認証サーバ。

【請求項 2 0】 前記登録手段は、前記受信者ホストまたは前記中継装置のアドレスとともに、当該受信者ホストまたは当該中継装置が接続されている所定ポートの情報を登録することを特徴とする請求項 1 7 ～ 1 9 の少なくとも一つに記載の認証サーバ。

【請求項 2 1】 前記登録手段は、前記受信者ホストまたは前記中継装置のアドレスとともに、前記参加申し込みを行った前記マルチキャストグループのグループアドレスを登録することを特徴とする請求項 1 7 ～ 2 0 の少なくとも一つに記載の認証サーバ。

【請求項 2 2】 前記登録手段は、前記マルチキャストグループへの前記受信者ホストの参加を許可する許可時間をさらに登録することを特徴とする請求項 1 7 ～ 2 1 の少なくとも一つに記載の認証サーバ。

【請求項 2 3】 前記認証サーバは、前記参加申し込みの際に、前記受信者ホストによって指定された前記マルチキャストグループへの参加時間に基づいて、前記許可時間を設定して前記登録手段に登録させる制御手段をさらに備えることを特徴とする請求項 1 7 ～ 2 2 の少なくとも一つに記載の認証サーバ。

【請求項 2 4】 前記認証サーバは、前記参加申し込みの際に、前記受信者ホストによって指定された前記マルチキャストグループに基づいて、前記許可時間を前記登録手段に登録させる制御手段をさらに備えたことを特徴とする請求項 1 7 ～ 2 2 の少なくとも一つに記載の認証サーバ。

【請求項 2 5】 前記登録手段は、前記受信者ホストまたは中継装置のアドレスと、前記マルチキャストグループのグループアドレスとの組を一つのユーザネームとして登録し、前記認証手段は、前記参加要求メッセージに含まれる送信元アドレスとグループアドレスの組を一つのユーザネームとして、前記登録手段の登録内容を検索して前記受信者ホストまたは中継装置の認証を行うことを特徴とする請求項 2 1 ～ 2 4 の少なくとも一つに記載の認証サーバ。

【請求項 2 6】 前記送信手段は、前記受信者ホストからの参加要求のメッセージに対し、前記登録手段の登録内容を送信することを特徴とする請求項 1 9 ～ 2 5 の少なくとも一つに記載の認証サーバ。

【請求項 2 7】 複数の受信者ホストと接続されるとともに、送信者ホスト



のネットワーク網を介して認証サーバと接続されるネットワーク間接続装置において、

前記受信者ホストから受信した参加要求のメッセージの送信元アドレスを抽出して、認証情報を問い合わせるメッセージを作成し、前記認証サーバに送信処理する送信処理手段と、

前記認証サーバから受信した認証結果のメッセージに基づいて、前記マルチキャストグループへの前記参加を許可する許可手段とを備えたことを特徴とするネットワーク間接続装置。

【請求項 28】 前記ネットワーク間接続装置は、前記マルチキャストグループの受信者を管理するための管理テーブルをさらに備え、

前記送信処理手段は、前記抽出した送信元アドレスのエントリが前記管理テーブルに存在するか判断し、該判断結果に基づいて、前記認証情報を問い合わせるメッセージを送信することを特徴とする請求項 27 に記載のネットワーク間接続装置。

【請求項 29】 前記送信処理手段は、前記受信した参加要求のメッセージの送信元アドレスとともにグループアドレスを抽出して、認証情報を問い合わせるメッセージを作成し、前記認証サーバに送信処理することを特徴とする請求項 27 または 28 に記載のネットワーク間接続装置。

【請求項 30】 前記許可手段では、前記認証サーバから受信した認証結果のメッセージに基づいて、許可時間内での前記マルチキャストグループへの前記参加を許可することを特徴とする請求項 27 または 28 に記載のネットワーク間接続装置。

【請求項 31】 前記許可手段では、前記認証サーバでの認証結果が認証の失敗の場合には、前記管理テーブルに登録されている該当するエントリを削除することを特徴とする請求項 28 または 30 に記載のネットワーク間接続装置。

【請求項 32】 前記送信者ホストは、インターネットのサービス事業者であり、前記ネットワーク網内にコンテンツのストリーム配信を行う配信サーバを備え、前記ネットワーク間接続装置の許可手段は、前記配信サーバから配信されるストリームのパケットを、前記許可された受信者ホストへマルチキャストフォ

ワーディングすることを特徴とする請求項 2 7 または 3 1 に記載のネットワーク間接続装置。

【請求項 3 3】 前記送信者ホストは、インターネットのサービス事業者であり、前記ネットワーク網内にコンテンツのストリーム配信を行う配信サーバを備え、前記ネットワーク間接続装置の許可手段は、前記許可時間内に前記配信サーバから配信されるストリームのパケットを、前記許可された受信者ホストへマルチキャストフォワーディングすることを特徴とする請求項 3 1 または 3 2 に記載のネットワーク間接続装置。

【請求項 3 4】 複数の受信者ホストと、送信者ホストのネットワーク網と、前記受信者ホストと前記ネットワーク網を接続させるネットワーク間接続装置と、前記ネットワーク網内に配設される認証サーバとを有するマルチキャスト認証システムにおいて、

前記認証サーバは、請求項 1 7 ～ 2 6 のいずれか一つに記載の認証サーバからなり、前記ネットワーク間接続装置は、請求項 2 7 ～ 3 3 のいずれか一つに記載のネットワーク間接続装置からなり、前記認証サーバによって前記送信者ホストのマルチキャストグループへの参加を認証し、前記ネットワーク間接続装置によって前記マルチキャストグループへの当該受信者ホストの参加を許可することを特徴とするマルチキャスト認証システム。

【請求項 3 5】 前記マルチキャスト認証システムは、ネットワーク間接続装置と受信者ホストとの間に接続される中継装置を有し、該中継装置は、前記受信者ホストから送信される参加要求のメッセージの送信元アドレスを自装置のアドレスに変更して前記ネットワーク間接続装置に中継するとともに、前記ネットワーク間接続装置から送信されるパケットの自装置宛の宛先アドレスを、前記参加要求を行った受信者ホストのアドレスに変更して中継することを特徴とする請求項 3 4 に記載のマルチキャスト認証システム。

【請求項 3 6】 前記マルチキャスト認証システムは、前記ネットワーク網内に配設され、コンテンツのストリーム配信を行う配信サーバをさらに有し、前記配信サーバから配信されるストリームのパケットを、前記許可された受信者ホストへマルチキャストフォワーディングすることを特徴とする請求項 3 4 または

35に記載のマルチキャスト認証システム。

【請求項37】 前記マルチキャスト認証システムでは、前記配信サーバから配信されるストリームのパケットを、許可時間内に前記許可された受信者ホストへマルチキャストフォワーディングすることを特徴とする請求項36に記載のマルチキャスト認証システム。

【請求項38】 前記マルチキャスト認証システムは、前記ネットワーク網内に配設され、実行されたサービスに応じた課金を行う課金サーバをさらに有し、前記ネットワーク間接続装置は、マルチキャストのストリームを検出し、検出データを前記課金サーバに送信することを特徴とする請求項34～37の少なくとも一つに記載のマルチキャスト認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、送信者ホストのマルチキャストグループへの受信者ホストの参加を認証するマルチキャスト認証方法、その認証サーバ、ネットワーク間接続装置およびマルチキャスト認証システムに関し、特に送信者ホストがインターネットのサービス事業者である場合の受信者ホストの参加を認証するマルチキャスト認証方法、その認証サーバ、ネットワーク間接続装置およびマルチキャスト認証システムに関するものである。

【0002】

【従来の技術】

従来のマルチキャスト認証方法は、IETF (Internet Engineering Task Force) により標準化されており、例えば図25のマルチキャスト認証システムの構成図に示すように、パソコンなどの受信者となるホスト（以下、「受信者ホスト」という）10、11と、マルチキャストグループのストリームを配信するバックボーンネットワーク13上の送信者となるホスト（以下、「送信者ホスト」という）14とを、ネットワーク間接続装置であるルータ12を介して接続させるものがあった。

【0003】

このシステムでは、受信者ホスト 1 0, 1 1 とルータ 1 2 間は、I G M P (Internet Group Management Protocol) によるメッセージの送受信を行っている。この I G M P は、R F C 2 2 3 6 で標準の方式となっており、受信者ホスト 1 0, 1 1 は、受信したいマルチキャストグループのアドレスを I G M P のパケットによってルータ 1 2 に通知し、ルータ 1 2 は、このような I G M P を受信したポート P 0, P 1 にだけ、送信者ホスト 1 4 から送信されるマルチキャストパケットのストリームをフォワードすることにより、必要な受信者ホスト 1 0, 1 1 にだけマルチキャストパケットを中継していた。

## 【 0 0 0 4 】

## 【発明が解決しようとする課題】

しかしながら、上記従来例に用いられる I G M P には、ユーザの認証の仕組みがないため、受信者ホスト 1 0, 1 1 から I G M P メッセージを受信したルータは、送信者ホスト 1 4 からのマルチキャストのストリームを無条件でフォワードすることとなる。

## 【 0 0 0 5 】

このため、たとえば企業内の L A N 環境においては、特に利用を制限することのない場合には問題とならないが、インターネットのサービス事業者のネットワークにおいて、有料のコンテンツなどを配信するような場合には、サービス事業者からフォワードされるマルチキャストのストリームを、受信者からの要求によって誰でも受信できる状況では、受信者を正確に認識できないという問題点があり、不正アクセスや課金などの面からも受信者の確認ができないことは問題であった。

## 【 0 0 0 6 】

また、1 9 9 9 年 2 月に発信されたインターネット・ドラフト「I P マルチキャスト・セnder、およびレシーバーの認証のための I G M P 拡張」(作成者 Norihiro 石川)では、受信者の認証を行うための I G M P の拡張が提案されているが、この提案では、受信者側のホストの機能も拡張しなければならず、既存の機能をそのまま使用することができないという問題点があった。

## 【 0 0 0 7 】

この発明は、上記問題点に鑑みなされたもので、受信者側のホストの機能は既存の仕組みのままで、ユーザを正確に認証できるマルチキャスト認証方法、その認証サーバ、ネットワーク間接続装置およびマルチキャスト認証システムを提供することを目的とする。

#### 【0008】

##### 【課題を解決するための手段】

上記目的を達成するため、この発明では、複数のホストと送信ホストのネットワーク網とがネットワーク間接続装置を介して接続されるとともに、前記ネットワーク網内の認証サーバによって前記送信ホストのマルチキャストグループへの参加を認証するマルチキャスト認証方法において、前記受信者ホストからの前記送信者ホストのマルチキャストグループへの参加申し込みに応じて、当該受信者ホストのアドレスを前記認証サーバに登録する登録工程と、前記受信者ホストからの参加要求のメッセージに対し、前記認証サーバの登録内容に基づいて受信者ホストの認証を行う認証工程とを含むことを特徴とする。

#### 【0009】

この発明によれば、参加申し込みにより、予めマルチキャストグループに参加できる受信者ホストを認証サーバに登録しておき、IGMPを用いて、受信者ホストから参加要求を示すメンバーシップ・レポートが送信されると、このレポート内の情報とこの認証サーバの登録内容に基づいて受信者ホストの認証がなされることにより、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証する。

#### 【0010】

この発明の請求項2では、複数の受信者ホストと送信者ホストのネットワーク網とがネットワーク間接続装置および中継装置を介して接続されるとともに、前記ネットワーク網内の認証サーバによって前記送信者ホストのマルチキャストグループへの参加を認証するマルチキャスト認証方法において、前記受信者ホストから前記送信者ホストのマルチキャストグループへの参加申し込みに応じて、当該受信者ホストが接続されている前記中継装置のアドレスを前記認証サーバに登録する登録工程と、前記受信者ホストからの参加要求のメッセージに対し、前記

認証サーバの登録内容に基づいて前記中継装置の認証を行う認証工程とを含むことを特徴とする。

## 【0011】

この発明によれば、参加申し込みにより、予めマルチキャストグループに参加できる受信者ホストが接続されている中継装置を認証サーバに登録しておき、IGMPを用いて、受信者ホストから参加要求を示すメンバーシップ・レポートが送信されると、このレポート内の情報とこの認証サーバの登録内容に基づいて中継装置の認証がなされることにより、受信者ホストの機能は既存の仕組みのまま、受信者ホストを正確に認証する。

## 【0012】

この発明の請求項3では、上記発明において、前記マルチキャスト認証方法では、前記参加要求のメッセージに対して前記受信者ホストの認証がなされると、前記マルチキャストグループへの当該受信者ホストの参加を許可する許可工程をさらに含むことを特徴とする。

## 【0013】

この発明によれば、認証されるとマルチキャストグループへの当該受信者ホストの参加を許可することにより、受信者ホストの認証後に、マルチキャストグループへのこの受信者ホストの参加が可能となる。

## 【0014】

この発明の請求項4では、上記発明において、前記登録工程では、前記受信者ホストまたは前記中継装置のアドレスとともに、当該受信者ホストまたは当該中継装置が接続されている前記ネットワーク間接続装置のポートの情報を前記認証サーバに登録することを特徴とする。

## 【0015】

自己のアドレスではない任意のアドレスによって参加を試みる受信者ホストに対して、ネットワーク間接続装置のポートの情報を認証サーバに登録することにより、不正なアクセスを防ぐ。

## 【0016】

この発明の請求項5では、上記発明において、前記登録工程では、前記マルチ

キャストグループのグループアドレスをさらに前記認証サーバに登録し、前記認証工程では、前記受信者ホストからの参加要求のメッセージに対し、前記認証サーバの登録内容に基づいて前記受信者ホストまたは前記中継装置と前記マルチキャストグループの認証を行うことを特徴とする。

## 【0017】

この発明によれば、受信者ホストまたは中継装置のアドレスとともにグループアドレスによってユーザの認証がなされることにより、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証する。

## 【0018】

この発明の請求項6では、上記発明において、前記登録工程では、全ての前記マルチキャストグループへの参加の申し込みに応じて、前記受信者ホストのアドレスを前記認証サーバに登録し、前記許可工程では、前記参加要求のメッセージに対して前記受信者ホストの認証がなされると、全ての前記マルチキャストグループへの当該受信者ホストの参加を許可することを特徴とする。

## 【0019】

この発明によれば、グループアドレスの指定のない受信者アドレスによる参加の申し込みの場合には、全てのマルチキャストの参加の申し込みと判断し、認証がなされると全てのマルチキャストグループへの当該受信者ホストの参加を許可することにより、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証する。

## 【0020】

この発明の請求項7では、上記発明において、前記登録工程では、前記マルチキャストグループへの参加を許可する許可時間をさらに前記認証サーバに登録し、前記許可工程では、参加要求のメッセージに対して前記受信者ホストの認証がなされると、前記許可時間内での前記マルチキャストグループへの当該受信者ホストの参加を許可することを特徴とする。

## 【0021】

この発明によれば、認証されると許可時間内でのマルチキャストグループへの当該受信者ホストの参加を許可することにより、受信者ホストの機能は既存の仕

組みのままで、受信者ホストを正確に認証する。

【 0 0 2 2 】

この発明の請求項 8 では、上記発明において、前記登録工程では、前記受信者ホストまたは中継装置のアドレスと、前記マルチキャストグループのグループアドレスとの組を一つのユーザネームとして登録し、前記認証工程では、前記参加要求メッセージに含まれる送信元アドレスとグループアドレスを抽出し、当該送信元アドレスとグループアドレスの組を一つのユーザネームとして、前記認証サーバの登録内容を検索して前記受信者ホストまたは中継装置の認証を行うことを特徴とする。

【 0 0 2 3 】

この発明によれば、送信元アドレスとグループアドレスの組を個別のユーザネームとすることで、マルチキャストグループごとのユーザの認証が可能となり、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証する。

【 0 0 2 4 】

この発明の請求項 9 では、上記発明において、前記許可工程では、前記許可時間は、前記マルチキャストグループごとに予め設定されており、前記参加申し込みの際に、前記受信者ホストによって指定された前記マルチキャストグループへの参加時間に基づいて、該受信者ホストに対する許可時間を設定して前記認証サーバに登録することを特徴とする。

【 0 0 2 5 】

この発明によれば、マルチキャストグループごとに参加を許可する許可時間が設定されており、ユーザが指定したマルチキャストグループへの参加時間に基づいて、前記許可時間が設定され、ユーザは時間になると、受信者ホストを起動させてマルチキャスト受信を開始できる。

【 0 0 2 6 】

この発明の請求項 1 0 では、上記発明において、前記許可工程では、前記許可時間は、前記マルチキャストグループごとに予め設定されており、前記参加申し込みの際に、前記受信者ホストによって指定された前記マルチキャストグループに基づいて、前記許可時間を前記認証サーバに登録することを特徴とする。



## 【 0 0 2 7 】

この発明によれば、マルチキャストグループごとに参加を許可する許可時間が予め設定されており、ユーザがマルチキャストグループを指定すると、その指定に基づいて、設定されている許可時間が自動的に認証サーバに登録されることとなり、ユーザは時間になると、受信者ホストを起動させてマルチキャスト受信を開始できる。

## 【 0 0 2 8 】

この発明の請求項 1 1 では、上記発明において、前記認証工程は、前記認証サーバが行い、認証結果とともに、前記受信者ホストがユーザ登録されている場合には、当該登録内容である許可時間の情報を前記ネットワーク間接続装置に送信し、前記許可工程は、前記ネットワーク間接続装置が行い、受信した前記認証結果に基づいて参加の許可を判断するとともに、受信した前記許可時間内での前記マルチキャストグループへの前記受信者ホストの参加を許可することを特徴とする。

## 【 0 0 2 9 】

この発明によれば、認証サーバが認証工程を行い、ネットワーク間接続装置が許可工程を行い、認証されると許可時間の情報がネットワーク間接続装置に送信され、ネットワーク間接続装置は、受信者ホストによる上記許可時間内でのマルチキャスト受信を許可する。

## 【 0 0 3 0 】

この発明の請求項 1 2 では、上記発明において、前記認証工程および許可工程は、前記ネットワーク間接続装置が行い、前記認証サーバは、前記参加申し込みの際に、指定された前記送信元アドレスとマルチキャストグループに対するユーザ登録内容を前記ネットワーク間接続装置に送信し、該ネットワーク間接続装置は、当該登録内容に基づいて前記受信者ホストの認証を行って、前記認証結果に基づいて参加の許可を判断するとともに、前記許可時間内での前記マルチキャストアドレスグループへの参加を許可することを特徴とする。

## 【 0 0 3 1 】

この発明によれば、ネットワーク間接続装置が認証工程と許可工程を行い、認

証サーバは、受信者ホストからの参加申し込みの際に登録したユーザ登録内容をネットワーク間接続装置に送信し、ネットワーク間接続装置は、この登録内容を受信者ホストから受信したアドレスに基づき、認証を行い、認証されると受信者ホストによる上記許可時間内でのマルチキャスト受信を許可する。

【 0 0 3 2 】

この発明の請求項 1 3 では、上記発明において、前記認証工程では、前記許可時間にならないと認証の失敗と判断することを特徴とする。

【 0 0 3 3 】

この発明によれば、上記許可時間になる前に、参加申し込みがなされた受信者ホストから参加要求のアクセスがあっても受け付けずに、認証の失敗と判断して許可時間内での再度のアクセスを待つものとする。

【 0 0 3 4 】

この発明の請求項 1 4 では、上記発明において、前記許可工程では、前記マルチキャストのユーザ登録を行い、前記認証工程で認証失敗と判断されると、該当するユーザ登録のエントリを削除することを特徴とする。

【 0 0 3 5 】

この発明によれば、ネットワーク間接続装置でのエントリがなくなり、参加要求の再アクセスに対しては認証工程での認証がなされ、認証されると受信者ホストによる上記許可時間内でのマルチキャスト受信を許可する。

【 0 0 3 6 】

この発明の請求項 1 5 では、上記発明において、前記送信者ホストは、インターネットのサービス事業者であり、該サービス事業者が配信サーバによるコンテンツのストリーム配信サービスを行っており、前記許可工程では、前記許可時間内に前記配信サーバから配信されるコンテンツのストリームを、前記認可された受信者ホストへマルチキャストフォワーディングすることを特徴とする。

【 0 0 3 7 】

この発明によれば、サービス事業者のネットワーク網に接続される受信者ホストからのストリームの配信サービスの参加申し込みに応じて、当該受信者ホストのアドレスとグループアドレスとともに、マルチキャストグループへの前記受信

者ホストの参加を許可する許可時間を認証サーバに登録し、認証されるとネットワーク間接続装置によって許可時間内に配信サーバからコンテンツのストリームが受信者ホストへマルチキャストフォワーディングされる。

【 0 0 3 8 】

この発明の請求項 1 6 では、上記発明において、実行されたサービスに応じて課金する課金工程をさらに含むことを特徴とする。

【 0 0 3 9 】

この発明によれば、例えばサービス事業者からのコンテンツのストリーム配信に際し、許可された時間内での時間配信に対してカウントを行って、そのカウント値に応じて課金される。

【 0 0 4 0 】

この発明の請求項 1 7 では、送信者ホストのネットワーク網内に設置される認証サーバにおいて、前記送信者ホストのネットワーク網に接続される受信者ホストからの前記送信者ホストのマルチキャストグループへの参加申し込みに応じて、当該受信者ホストのアドレスを登録する登録手段を備えたことを特徴とする。

【 0 0 4 1 】

この発明によれば、認証サーバでは、参加申し込み時に、受信者ホストのアドレスを登録手段に登録しており、当該受信者ホストからの参加要求に対する認証を可能にする。

【 0 0 4 2 】

この発明の請求項 1 8 では、送信者ホストのネットワーク網内に設置される認証サーバにおいて、中継装置を介して前記送信者ホストのネットワーク網に接続される受信者ホストからの前記送信者ホストのマルチキャストグループへの参加申し込みに応じて、当該中継装置のアドレスを登録する登録手段を備えたことを特徴とする。

【 0 0 4 3 】

この発明によれば、認証サーバでは、中継装置が介在している場合には、参加要求のメッセージの送信元が受信者ホストのアドレスから中継装置の当該受信者ホストが接続されているインターフェースの物理ポートのアドレスに変更される

ので、登録手段にも中継装置の上記物理ポートのアドレスを登録しており、当該受信者ホストからの参加要求に対する認証を可能にする。

## 【 0 0 4 4 】

この発明の請求項 1 9 では、上記発明において、前記認証サーバは、前記受信者ホストからの参加要求のメッセージに対し、前記登録手段の登録内容に基づいて参加の認証を行う認証手段と、前記認証結果を送信する送信手段とをさらに備えたことを特徴とする。

## 【 0 0 4 5 】

この発明によれば、認証サーバでは、登録手段の他に、認証手段と送信手段を備え、参加要求のメッセージの送信元アドレスに対し、登録内容に基づいて参加の認証を行い、その認証結果をネットワーク間接続装置に送信し、上記ネットワーク間接続装置による参加の許可判定を可能にする。

## 【 0 0 4 6 】

この発明の請求項 2 0 では、上記発明において、前記登録手段は、前記受信者ホストまたは前記中継装置のアドレスとともに、当該受信者ホストまたは当該中継装置が接続されている所定ポートの情報を登録することを特徴とする。

## 【 0 0 4 7 】

自己のアドレスではない任意のアドレスによって参加を試みる受信者ホストに対して、ネットワーク間接続装置のポートの情報を認証サーバの登録手段に登録することにより、不正なアクセスを防ぐ。

## 【 0 0 4 8 】

この発明の請求項 2 1 では、上記発明において、前記登録手段は、前記受信者ホストまたは前記中継装置のアドレスとともに、前記参加申し込みを行った前記マルチキャストグループのグループアドレスを登録することを特徴とする。

## 【 0 0 4 9 】

この発明によれば、受信者ホストまたは中継装置のアドレスとともにグループアドレスが登録され、これらアドレスによってユーザの認証が可能となり、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証することができる。

## 【 0 0 5 0 】

この発明の請求項 2 2 では、上記発明において、前記登録手段は、前記マルチキャストグループへの前記受信者ホストの参加を許可する許可時間をさらに登録することを特徴とする。

## 【 0 0 5 1 】

この発明によれば、マルチキャストグループへの参加を許可する許可時間も登録されており、上記アドレスおよび許可時間によってユーザの認証が可能となり、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証することができる。

## 【 0 0 5 2 】

この発明の請求項 2 3 では、上記発明において、前記認証サーバは、前記参加申し込みの際に、前記受信者ホストによって指定された前記マルチキャストグループへの参加時間に基づいて、前記許可時間を設定して前記登録手段に登録させる制御手段をさらに備えることを特徴とする。

## 【 0 0 5 3 】

この発明によれば、ユーザがマルチキャストグループへの参加時間を指定することにより、制御手段がユーザの当該マルチキャストグループへの参加の許可時間を登録手段に登録させて、ユーザからの参加要求に備える。

## 【 0 0 5 4 】

この発明の請求項 2 4 では、上記発明において、前記認証サーバは、前記参加申し込みの際に、前記受信者ホストによって指定された前記マルチキャストグループに基づいて、前記許可時間を前記登録手段に登録させる制御手段をさらに備えたことを特徴とする。

## 【 0 0 5 5 】

この発明によれば、ユーザがマルチキャストグループを指定することにより、制御手段が予め設定されているユーザの参加の許可時間を登録手段に登録させて、ユーザからの参加要求に備える。

## 【 0 0 5 6 】

この発明の請求項 2 5 では、上記発明において、前記登録手段は、前記受信者

ホストまたは中継装置のアドレスと、前記マルチキャストグループのグループアドレスとの組を一つのユーザネームとして登録し、前記認証手段は、前記参加要求メッセージに含まれる送信元アドレスとグループアドレスの組を一つのユーザネームとして、前記登録手段の登録内容を検索して前記受信者ホストまたは中継装置の認証を行うことを特徴とする。

## 【 0 0 5 7 】

この発明によれば、認証サーバでは、登録手段に登録されているユーザのアドレスとグループアドレスとの組からなるユーザネームと許可時間などの登録内容を、認証手段が参加要求メッセージの送信元アドレスとグループアドレスの組からなるユーザネームで検索してユーザの認証を行うことで、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証することができる。

## 【 0 0 5 8 】

この発明の請求項 2 6 では、上記発明において、前記送信手段は、前記受信者ホストからの参加要求のメッセージに対し、前記登録手段の登録内容を送信することを特徴とする。

## 【 0 0 5 9 】

この発明によれば、認証サーバでは、ネットワーク間接続装置を介して入力する受信者ホストからの参加要求のメッセージに対し、登録内容を送信し、認証後の参加許可、たとえばコンテンツのストリーム配信を可能にする。

## 【 0 0 6 0 】

この発明の請求項 2 7 では、複数の受信者ホストと接続されるとともに、送信者ホストのネットワーク網を介して認証サーバと接続されるネットワーク間接続装置において、前記受信者ホストから受信した参加要求のメッセージの送信元アドレスを抽出して、認証情報を問い合わせるメッセージを作成し、前記認証サーバに送信処理する送信処理手段と、前記認証サーバから受信した認証結果のメッセージに基づいて、前記マルチキャストグループへの前記参加を許可する許可手段とを備えたことを特徴とする。

## 【 0 0 6 1 】

この発明によれば、ネットワーク間接続装置では、送信処理手段が参加要求メ

ッセージから送信元アドレスを抽出し、認証を問い合わせるメッセージを送信し、その認証結果のメッセージを認証サーバから受信し、認証された場合には、許可手段でグループ参加を許可する。

## 【 0 0 6 2 】

この発明の請求項 2 8 によれば、上記発明において、前記ネットワーク間接続装置は、前記マルチキャストグループの受信者を管理するための管理テーブルをさらに備え、前記送信処理手段は、前記抽出した送信元アドレスのエントリが前記管理テーブルに存在するか判断し、該判断結果に基づいて、前記認証情報を問い合わせるメッセージを送信することを特徴とする。

## 【 0 0 6 3 】

この発明によれば、ネットワーク間接続装置では、メッセージから抽出した送信元アドレスとグループアドレスのエントリが、管理テーブルにない場合に、認証情報を認証サーバに問い合わせる。

## 【 0 0 6 4 】

この発明の請求項 2 9 によれば、上記発明において、前記送信処理手段は、前記受信した参加要求のメッセージの送信元アドレスとともにグループアドレスを抽出して、認証情報を問い合わせるメッセージを作成し、前記認証サーバに送信処理することを特徴とする。

## 【 0 0 6 5 】

この発明によれば、ネットワーク間接続装置では、送信処理手段が参加要求メッセージから送信元アドレスとグループアドレスを抽出し、認証を問い合わせるメッセージを送信する。

## 【 0 0 6 6 】

この発明の請求項 3 0 では、上記発明において、前記許可手段では、前記認証サーバから受信した認証結果のメッセージに基づいて、許可時間内での前記マルチキャストグループへの前記参加を許可することを特徴とする。

## 【 0 0 6 7 】

この発明によれば、認証結果のメッセージを認証サーバから受信し、認証された場合には、許可手段で許可時間内でのグループ参加を許可する。

## 【 0 0 6 8 】

この発明の請求項 3 1 では、上記発明において、前記許可手段では、前記認証サーバでの認証結果が認証の失敗の場合には、前記管理テーブルに登録されている該当するエントリを削除することを特徴とする。

## 【 0 0 6 9 】

この発明によれば、ネットワーク間接続装置では、管理テーブルのエントリがなくなり、参加要求の再アクセスに対して認証サーバでの認証が行われるようにする。

## 【 0 0 7 0 】

この発明の請求項 3 2 では、上記発明において、前記送信者ホストは、インターネットのサービス事業者であり、前記ネットワーク網内にコンテンツのストリーム配信を行う配信サーバを備え、前記ネットワーク間接続装置の許可手段は、前記配信サーバから配信されるストリームのパケットを、前記許可された受信者ホストへマルチキャストフォワーディングすることを特徴とする。

## 【 0 0 7 1 】

この発明によれば、送信者ホストがサービス事業者の場合に、ネットワーク間接続装置の許可手段では、配信されるストリームのパケットを許可された受信者ホストにマルチキャストフォワーディングする。

## 【 0 0 7 2 】

この発明の請求項 3 3 では、上記発明において、前記送信者ホストは、インターネットのサービス事業者であり、前記ネットワーク網内にコンテンツのストリーム配信を行う配信サーバを備え、前記ネットワーク間接続装置の許可手段は、前記許可時間内に前記配信サーバから配信されるストリームのパケットを、前記許可された受信者ホストへマルチキャストフォワーディングすることを特徴とする。

## 【 0 0 7 3 】

この発明によれば、送信者ホストがサービス事業者の場合に、ネットワーク間接続装置の許可手段では、配信されるストリームのパケットを許可時間内受信者ホストにマルチキャストフォワーディングする。



## 【 0 0 7 4 】

この発明の請求項 3 4 では、複数の受信者ホストと、送信者ホストのネットワーク網と、前記受信者ホストと前記ネットワーク網を接続させるネットワーク間接続装置と、前記ネットワーク網内に配設される認証サーバとを有するマルチキャスト認証システムにおいて、前記認証サーバは、請求項 1 7 ～ 2 6 のいずれか一つに記載の認証サーバからなり、前記ネットワーク間接続装置は、請求項 2 7 ～ 3 3 のいずれか一つに記載のネットワーク間接続装置からなり、前記認証サーバによって前記送信者ホストのマルチキャストグループへの参加を認証し、前記ネットワーク間接続装置によって前記マルチキャストグループへの当該受信者ホストの参加を許可することを特徴とする。

## 【 0 0 7 5 】

この発明によれば、認証サーバとネットワーク間接続装置とを各請求項に記述したごとく、特徴を持たせて、マルチキャストグループへの参加認証や許可時間内での例えば配信サービスを行うことで、受信者ホストの機能は既存の仕組みのまま、ユーザを正確に認証できる。

## 【 0 0 7 6 】

この発明の請求項 3 5 では、前記マルチキャスト認証システムは、ネットワーク間接続装置と受信者ホストとの間に接続される中継装置を有し、該中継装置は、前記受信者ホストから送信される参加要求のメッセージの送信元アドレスを自装置のアドレスに変更して前記ネットワーク間接続装置に中継するとともに、前記ネットワーク間接続装置から送信されるパケットの自装置宛の宛先アドレスを、前記参加要求を行った受信者ホストのアドレスに変更して中継することを特徴とする。

## 【 0 0 7 7 】

この発明によれば、ネットワーク間接続装置と受信者ホストとの間に中継装置が接続されている場合、中継装置では、参加要求メッセージの送信元アドレスを自装置のアドレスに、パケットの宛先アドレスを許可された受信者ホストのアドレスに変換してそれぞれ中継することで、プロキシ機能を持った中継装置が介在しても、参加の認証を行うことができ、認証されると許可時間内でのマルチキャ

ストグループへの当該受信者ホストの参加を許可することにより、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証する。

【 0 0 7 8 】

この発明の請求項 3 6 では、前記マルチキャスト認証システムは、前記ネットワーク網内に配設され、コンテンツのストリーム配信を行う配信サーバをさらに有し、前記配信サーバから配信されるストリームのパケットを、前記許可された受信者ホストへマルチキャストフォワーディングすることを特徴とする。

【 0 0 7 9 】

この発明によれば、サービス事業者の提供するサービスが配信サーバを用いたコンテンツのストリーム配信サービスの場合、配信されるストリームのパケットを受信者ホストへマルチキャストフォワーディングする。

【 0 0 8 0 】

この発明の請求項 3 7 では、上記発明において、前記マルチキャスト認証システムでは、前記配信サーバから配信されるストリームのパケットを、許可時間内に前記許可された受信者ホストへマルチキャストフォワーディングすることを特徴とする。

【 0 0 8 1 】

この発明によれば、サービス事業者の提供するサービスが配信サーバを用いたコンテンツのストリーム配信サービスの場合、配信されるストリームのパケットを許可時間内受信者ホストへマルチキャストフォワーディングする。

【 0 0 8 2 】

この発明の請求項 3 8 では、上記発明において、前記マルチキャスト認証システムは、前記ネットワーク網内に配設され、実行されたサービスに応じた課金を行う課金サーバをさらに有し、前記ネットワーク間接続装置は、マルチキャストのストリームを検出し、検出データを前記課金サーバに送信することを特徴とする。

【 0 0 8 3 】

この発明によれば、課金サーバは、実行されたサービスに応じて定額制または従量制で課金しており、例えばコンテンツの配信サービスの場合には、定額制の

課金ではいつ申し込んでもコンテンツの配信が受けられ、従量制の課金では認証の後、実際にマルチキャストのストリームが流れた時点でネットワーク間接続装置がストリーム配信を検出し、課金サーバに課金に必要な検出データを送信する。

【0084】

【発明の実施の形態】

以下に添付図面を参照して、この発明に係るマルチキャスト認証方法、その認証サーバ、ネットワーク間接続装置およびマルチキャスト認証システムの好適な実施の形態を説明する。なお、図25と同様の構成部分に関しては、説明の都合上、同一符号を付記するものとする。

【0085】

(概略構成)

図1は、この発明にかかるマルチキャスト認証システムの概略構成を示す構成図である。図1において、図25の構成と異なる点は、バックボーンネットワーク13上にユーザ認証サーバ15を配設する点であり、ユーザ認証サーバ15には、例えば予めWebページで公開されたコンテンツの配信予定などの申し込みに対して、ユーザが入力したユーザ情報（アドレス）や参加を希望するコンテンツ（マルチキャストグループ）のグループアドレスや受信者ホスト10、11が接続されるPEルータ12のポートの情報がデータベースとして登録されている。

【0086】

ここで、例えば送信者ホスト14から配信されるコンテンツに対して、受信者ホスト10、11からは、送信元アドレスを自己のIPアドレスとして、このコンテンツに参加を希望する旨の申し込みの通知を行えば、受信者ホストのアドレスがユーザ認証サーバ15に登録される。

【0087】

そして、次に受信者ホストが参加要求を行うことによって、ユーザ認証サーバ15は、PEルータ12を介して送られてくる上記参加要求のメッセージ内の送信元アドレスから、登録されているアドレスを検索し、一致すればそこで認証が

なされ、送信者ホスト 1 4 から常時コンテンツの配信が受けられることとなる。

## 【 0 0 8 8 】

しかし、送信者ホスト 1 4 から配信されるコンテンツは、1 種類に限らず、実際には複数の種類が存在する。そこで、コンテンツ毎の受信者ホストの認証が必要になる場合がある。この場合には、受信者ホストは、配信が予定されている各マルチキャストグループのうちから、参加を希望する特定のマルチキャストグループのグループアドレスを指定することによって、ユーザ認証サーバ 1 5 のマルチキャスト受信者認証テーブルに登録される。

## 【 0 0 8 9 】

この場合も、受信者ホストが参加要求を行うことによって、ユーザ認証サーバ 1 5 は、P E ルータ 1 2 を介して送られてくる上記参加要求のメッセージ内の送信元アドレスとグループアドレスから、登録されているアドレスを検索し、一致すればそこで認証がなされ、送信者ホスト 1 4 から常時コンテンツの配信が受けられることとなる。

## 【 0 0 9 0 】

また、受信者ホストからは、この特定のマルチキャストグループのグループアドレスを指定しないで、参加要求を行うことも可能である。ただし、この場合には、全てのマルチキャストグループの指定となって、ユーザ認証サーバ 1 5 のマルチキャスト受信者認証テーブルに登録される。

## 【 0 0 9 1 】

この場合には、受信者ホストが参加要求を行うことによって、ユーザ認証サーバ 1 5 は、P E ルータ 1 2 を介して送られてくる上記参加要求のメッセージ内の送信元アドレスから、登録されているアドレスを検索し、一致すればそこで認証がなされ、送信者ホスト 1 4 から常時複数のコンテンツの配信が受けられることとなる。

## 【 0 0 9 2 】

また、自己の I P アドレスではない任意の I P アドレスによってマルチキャストグループへの参加を試みる受信者ホストに対しては、上記の認証では不正参加を防ぐことができないので、例えば受信者ホスト 1 0, 1 1 が接続されている P

E ルータ 1 2 のポートの情報を、認証の対象にすることも可能である。

【 0 0 9 3 】

この場合には、受信者ホストが参加要求を行うことによって、ユーザ認証サーバ 1 5 は、P E ルータ 1 2 を介して送られてくる上記参加要求のメッセージ内の送信元アドレスとポートの情報から、登録されているアドレスを検索し、一致すればそこで認証がなされ、送信者ホスト 1 4 から常時複数のコンテンツの配信が受けられることとなる。

【 0 0 9 4 】

なお、この発明におけるポートの情報とは、受信者ホストが実際に接続されている物理ポートの情報に限らず、例えば論理ポートの情報でも良い。この場合には、論理ポートに属する物理ポート以外の物理ポートからの不正アクセスを防ぐことができる。

【 0 0 9 5 】

さらに、配信されるコンテンツの中には、例えば音楽やスポーツの試合のライブ配信のようにリアルタイムで行われるものもあり、このようなライブ配信では、そのライブが開催される時間を特定することも可能となる。そこで、上述のデータに対応させてコンテンツの配信を行う許可時間を登録させることが可能となる。

【 0 0 9 6 】

これらの認証の対象となる項目については、使用状況などに応じて、適宜組み合わせる用いることができる。また、上記の認証は、一般的にはユーザ認証サーバ 1 5 で行うが、例えば P E ルータ 1 2 にその機能をもたせることも可能である。

【 0 0 9 7 】

図 2 は、このユーザ認証サーバ 1 5 のマルチキャスト受信者認証テーブルの構成を示す構成図である。図において、このマルチキャスト受信者認証テーブルには、受信者ホストの I P アドレスである受信者 I P アドレスと、その受信者ホストが参加するマルチキャストグループのグループアドレスと、受信者ホストが接続される P E ルータ 1 2 のポートの I P アドレスと、その P E ルータポート番号

が格納されている。

#### 【0098】

この構成例では、例えば受信者ホスト10、11の受信者IPアドレスを“192.52.150.1”、“192.52.122.1”とし、受信者ホスト10が配信を受けるマルチキャストグループのグループアドレスを“224.1.1.1”とし、受信者ホスト11が配信を受けるマルチキャストグループを全てのグループとした場合を示している。また、この構成例では、受信者ホスト10が接続されるPEルータ12のポートのPEルータIPアドレスを“220.0.0.1”、そのポート番号を“1”とし、受信者ホスト11が接続されるPEルータ12のポートのPEルータIPアドレスを“220.0.0.2”、そのポート番号を“6”としている。

#### 【0099】

このような構成において、図3のタイムチャートに示すように、受信者ホスト10、11は、受信したいマルチキャストグループのグループアドレス（ただし、受信者ホスト11の場合には、グループアドレスなし）をIGMPのメンバーシップ・レポートのメッセージに付加してルータ12に送信する。ルータ12は、このレポートを受信すると、その受信者ホストの送信元アドレスと参加要求しているマルチキャストグループのグループアドレスを抽出してユーザ認証サーバ15に問い合わせる。

#### 【0100】

なお、この問い合わせは、例えば後述するRADIUSメッセージによってなされる。この問い合わせの際には、後述するRADIUSメッセージの種類を示すコード（code）が、「Access-Request」のメッセージを送信する。このメッセージは、一旦認証がなされた場合でも、ルータ12が一定間隔、例えば10分間隔でユーザ認証サーバ15に対して送信されている。これは、例えばユーザが予約をキャンセルした場合などに対応するためであり、また課金する場合でも、このキャンセルに対応できるようにするためである。

#### 【0101】

また、時刻指定で配信予約した場合であっても、同様にキャンセルや変更があるので、これに対応するためには、認証後も定期的に「Access-Request

e s t」のメッセージを、ルータ 1 2 からユーザ認証サーバ 1 5 に送信して、ユーザ認証サーバ 1 5 内のマルチキャスト受信者認証テーブルをチェックし、応答させる必要性がある。

#### 【0 1 0 2】

ここで、IGMPのメンバーシップ・レポートメッセージのパケットフォーマットは、図4に示すように、レイヤ2レベルの送信元アドレスや宛先アドレスを格納するMACヘッダと、レイヤ3レベルの送信元アドレスや宛先アドレスを格納するIPヘッダと、IGMP Messageとから構成されており、IGMP Messageは、図5のフォーマットに示すように、メッセージのタイプを示すTypeと、Max Resp Timeと、パケットチェック用のChecksumと、グループIPアドレスを格納するGroup Addressとから構成されている。

#### 【0 1 0 3】

なお、この実施例において、Typeは、バージョン2メンバーシップ・レポートを示す0x16の値からなり、Max Resp Timeは、0の値からなり、Checksumは、IGMPメッセージのチェックサム値(Checksum部分は0で計算)からなり、Group Addressには、受信者ホストが参加したいマルチキャストグループのアドレス(マルチキャストアドレス)が格納されている。

#### 【0 1 0 4】

この実施例では、図4に示したIPヘッダ内の受信者ホストの送信元アドレスと、図5に示したIGMP Message内のこの受信者ホストが参加要求しているマルチキャストグループのグループアドレスを抽出し、この送信元アドレスとグループアドレスの組を一つのユーザネームとして、次に説明するRADIUSメッセージを作成する。

#### 【0 1 0 5】

このRADIUSメッセージのパケットフォーマットは、図6に示すように、レイヤ2レベルの送信元アドレスや宛先アドレスを格納するMACヘッダと、レイヤ3レベルの送信元アドレスや宛先アドレスを格納するIPヘッダと、ラン

スポーツ層のUDPヘッダと、RADIUS Messageとから構成されている。

#### 【0106】

このRADIUS Messageは、図7に示すように、このメッセージの種類を示すCodeと、このメッセージを識別するIDであるIdentifierと、メッセージ長を示すLengthと、このメッセージを認証するデータ（例えばMD5のハッシュ）であるAuthenticatorと、属性値を示すAttributesとから構成されている。また、Attributesは、図8に示すように、属性の種類を示すTypeと、データ長であるLengthと、このTypeで示された実際の値を示すValueとから構成されている。

#### 【0107】

なお、ここで、図7に示したRADIUS MessageのCodeは、1の場合には、受信者ホストの送信元アドレスと参加要求しているマルチキャストグループのグループアドレスによる認証を問い合わせる「Access-Request」のRADIUSメッセージを示し、2の場合には、認証を許可する「Access-Accept」のRADIUSメッセージを示し、3の場合には、認証を許可しない「Access-Reject」のRADIUSメッセージを示し、4の場合には、経時時間のカウントを要求する「Accounting-Request」のRADIUSメッセージを示し、5の場合には、このカウントを応答する「Accounting-Response」のRADIUSメッセージを示している。

#### 【0108】

図7に示したAttributesのTypeは、図8に示すように、1の場合には、ユーザネームを示し、その時のValueには、実際の値、例えば受信者ホスト10のIPアドレスを“192.52.150.1”とし、グループIPアドレスを“224.1.1.1”とすると、Valueには、“192.52.150.1-224.1.1.1”の値が格納され、2の場合には、ユーザパスワードを示し、その時のValueには、例えば“RADIUS-CLIENT”の値が格納される。



【0109】

なお、全てのマルチキャストグループを指定する場合には、V a l u e には、受信者ホスト11のIPアドレス“192.52.122.1”の値のみが格納される。

【0110】

また、A t t r i b u t e s の T y p e において、4の場合には、P E ルータのポートのIPアドレスであるN A S - I P - A d d r e s s の値、例えば受信者ホスト10が接続されているP E ルータIPアドレスの値“220.0.0.1”が格納され、5の場合には、そのポートの番号であるN A S - P o r t の値、例えば“1”が格納されている。

【0111】

なお、受信者ホスト10とポートの情報を指定する場合には、上記のV a l u e には、受信者ホスト10のIPアドレス“192.52.150.1”の値のみが格納され、N A S - I P - A d d r e s s の値には“220.0.0.1”が、N A S - P o r t の値には“1”が格納される。

【0112】

また、A t t r i b u t e s の T y p e において、223の場合には、コンテンツの配信サービスを開始する時間、“Multicast-Time-Start”の値が格納され、224の場合には、コンテンツの配信サービスを終了する時間、“Multicast-Time-End”の値が格納されている。

【0113】

なお、この時間の情報は、上記の各指定と組み合わせて指定することができ、コンテンツの配信時間内などにユーザの認証を行うことが可能となる。

【0114】

ユーザ認証サーバ15は、この問い合わせのR A D I U S メッセージを受信すると、登録内容から受信者ホストのIPアドレスを確認し、そのマルチキャストグループへの参加を認証するかどうか判断し、この認証結果（および許可時間が設定されている場合には、そのマルチキャストグループへの参加許可時間）をルータ12に応答する。なお、この応答も、上記のR A D I U S メッセージによってなされており、この応答の際には、R A D I U S メッセージの種類を示すコー

ドが、認証を許可する場合には「Access-Accept」を、また認証が不許可の場合には「Access-Reject」のRADIUSメッセージをルータ12に送信する。

#### 【0115】

また、ユーザ認証サーバ15は、参加許可時間が設定されている場合には、この参加許可時間の前にこの問い合わせのRADIUSメッセージを受信した場合には、たとえ登録内容の受信者ホストであっても、認証の失敗と判断して、「Access-Reject」のRADIUSメッセージをルータ12に送信する。

#### 【0116】

ルータ12は、認証結果が認証を許可することを示す「Access-Accept」のメッセージを受信した場合には、通常のIGMP受信と同様の処理を行い、対応するマルチキャストのストリームを、参加許可された受信者ホストが接続されているインターフェースのポートに、フォワード（参加許可時間が設定されている場合には、上記参加許可時間内フォワード）する。また、認証結果が不許可することを示す「Access-Reject」のメッセージを受信した場合には、ルータ12は、受信者ホストからのIGMP受信がなかったものとして、対応するマルチキャストのストリームのフォワードは行わない。

#### 【0117】

このように、この発明では、IGMPのメンバーシップ・レポート内の情報と、予め登録された認証サーバの登録内容とに基づいて参加が許可されたユーザに対して、マルチキャストストリームの送信を行うので、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証でき、このため参加許可されないユーザがこのマルチキャストストリームを受信することを防ぐことが可能となり、これに伴ってマルチキャストを利用した有料ストリーム配信のサービスが可能となる。

#### 【0118】

また、この発明では、所定マルチキャストグループまたは全マルチキャストグループに参加が許可されたユーザに対して、当該グループのマルチキャストスト

リームの送信を行うので、上記と同様、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証でき、このため参加許可されないユーザがこのマルチキャストストリームを受信することを防ぐことが可能となり、これに伴ってマルチキャストを利用した有料ストリーム配信のサービスが可能となる。

## 【0119】

また、この発明では、所定ポートに接続された受信者ホストのユーザに対して、当該グループのマルチキャストストリームの送信を行うので、受信者ホストの機能は既存の仕組みのままで、受信者ホストをさらに正確に認証でき、このため参加許可されないユーザがこのマルチキャストストリームを受信することを防ぐことが可能となり、これに伴ってマルチキャストを利用した有料ストリーム配信のサービスが可能となる。

## 【0120】

さらに、この発明では、マルチキャストグループへの参加許可時間を認証の対象に設定し、参加が許可されたユーザに対して参加許可時間内のマルチキャストストリームの送信を行うので、参加許可されないユーザがこのマルチキャストストリームを受信することを防ぐことが可能となり、これに伴ってマルチキャストを利用した有料ストリーム配信のサービスが可能となる。

## 【0121】

次に、マルチキャスト認証システムの実施例について説明する。

## (実施例1)

## 【0122】

図9は、この発明にかかるマルチキャスト認証システムの実施例1の構成を示す構成図である。図において、このシステムは、複数のユーザPC（受信者ホスト）20、21と、ユーザPC20、21が接続される中継装置であるカスタマエッジルータ（以下、「CEルータ」という）22、23と、サービス事業者のIP網29に配設されるネットワーク間接続装置であるプロバイダエッジルータ（以下、「PEルータ」という）30と、同じくIP網29に配設されてストリームを配信するストリームコンテンツ配信サーバ31と、同じくIP網29に配設されてユーザPCの認証を行うユーザ認証サーバ32と、同じくIP網29に

配設されてユーザPCからの配信受付を行う配信受付サーバ33と、同じくIP網29に配設されて課金の計算を行う課金サーバ34とから構成されている。

#### 【0123】

CEルータ22, 23は、ユーザPC20, 21とPEルータ30との間に介在し、ユーザPC20, 21からPEルータ30へのIGMPメンバーシップレポートのメッセージパケットやユーザPC20, 21と配信受付サーバ33間のWebページ上でのデータの送受信を中継している。これらCEルータ22, 23は、互いに同一の構成になっているので、ここでは代表してCEルータ22の構成を図10に示す。図において、CEルータ22は、ユーザPC20やPEルータ30とポートを介して接続されるLANインタフェース22aと、LANインタフェース22aで取り込まれたパケットを受信し、パケットの種類を判別して振り分けるパケット受信部22bと、パケット受信部22bで振り分けられたIGMPメンバーシップレポートのメッセージパケットをIGMP Proxyの機能を用いて処理するIGMP Proxy処理部22cと、パケット受信部22bで振り分けられたマルチキャストパケットを中継処理するパケット中継処理部22dと、各処理部22c, 22dで処理されたパケットを送信するパケット送信部22eとから構成されている。IGMP Proxy処理部22cは、IGMP Proxyとして機能し、ユーザPC20からのパケットの中継時に送信元アドレスを、ユーザPC20のIPアドレスからCEルータ22のIPアドレスに変更している。

#### 【0124】

PEルータ30は、図11の構成図に示すように、各CEルータ22, 23や各種サーバ31~34とポートを介して接続されるLANインタフェース30aと、LANインタフェース30aで取り込まれたパケットを受信し、パケットの種類を判別して振り分けるパケット受信部30bと、パケット受信部30bで振り分けられたIGMPメンバーシップレポートのメッセージパケットの制御処理を行うIGMP制御部30cと、パケット受信部30bで振り分けられたRADIUSメッセージのパケットの制御処理を行う認証制御部30dと、パケット受信部30bで振り分けられたマルチキャストパケットのフォワーディング制御処

理を行うマルチキャストフォワーディング制御部 3 0 e と、各制御部 3 0 c ~ 3 0 e と接続されて、これらパケットから得られるマルチキャスト受信者の情報を格納するマルチキャスト受信者管理テーブル 3 0 f と、マルチキャストパケットをフォワーディングするためのルート情報を格納するマルチキャストフォワーディングテーブル 3 0 g と、各制御部 3 0 c ~ 3 0 e で処理されたパケットを送信するパケット送信部 3 0 h とから構成されている。

## 【 0 1 2 5 】

マルチキャスト受信者管理テーブル 3 0 f は、図 1 2 に示すように、ユーザ P C が参加を希望するマルチキャストグループのグループアドレスと、受信者 I P アドレスと、このユーザ P C が接続されるインターフェースの受信者ポート番号と、コンテンツの配信を行うストリームコンテンツ配信サーバ 3 1 が接続されるインターフェースの送信者ポート番号とから構成されている。なお、このシステムにおいて、P E ルータ 3 0 には I G M P P r o x y 機能を有する C E ルータ 2 2 , 2 3 が接続されているので、受信者 I P アドレスにはこの C E ルータ 2 2 , 2 3 の I P アドレス、例えば “201.1.1.1” と “201.1.1.2” とが格納されており、受信者ポート番号には、この C E ルータが接続されているインターフェースのポート番号が格納されている。この管理テーブル 3 0 f は、C E ルータ 2 2 , 2 3 との間で送受される I G M P メッセージの情報に基づいて作成される。

## 【 0 1 2 6 】

また、マルチキャストフォワーディングテーブルには、図 1 3 に示すように、ストリームコンテンツ配信サーバ 3 1 で配信されるコンテンツを示すマルチキャストグループのグループアドレスと、当該マルチキャストグループに参加を希望する各ユーザ P C ( C E ルータ ) が接続されるインターフェースの受信者ポート番号のリストが格納されている。

## 【 0 1 2 7 】

ユーザ認証サーバ 3 2 は、図 1 4 に示すように、P E ルータ 3 0 や配信受付サーバ 3 3 とポートを介して接続される L A N インタフェース 3 2 a と、L A N インタフェース 3 2 a で取り込まれた R A D I U S メッセージのパケットを受信するパケット受信部 3 2 b と、受信された R A D I U S メッセージ内の送信元アド

レスとグループアドレスに基づいてユーザの認証を行う認証制御部 3 2 c と、配信受付サーバ 3 3 に接続されて受け付けられたユーザ情報などが入力する配信受付サーバインタフェース 3 2 d と、配信受付サーバインタフェース 3 2 d から入力するユーザ情報を登録するマルチキャスト受信者認証テーブル 3 2 e と、認証制御部 3 2 c からの認証結果を LAN インタフェース 3 2 a を介して送信するパケット送信部 3 2 f とから構成されている。

#### 【 0 1 2 8 】

このユーザ認証サーバ 3 2 のマルチキャスト受信者認証テーブル 3 2 e は、上述した図 2 に示したような構成からなっている。また、ユーザ認証サーバ 3 2 は、users ファイルを有しており、この users ファイルは、ユーザネームの情報と、パスワード、例えば“RADIUS-CLIENT”の値と、拡張属性としてコンテンツの配信サービスを開始する時間である“Multicast-Time-Start”の値と、コンテンツの配信サービスを終了する時間である“Multicast-Time-End”の値とが格納されている。

#### 【 0 1 2 9 】

このユーザネームの情報は、受信者ホストの IP アドレスとグループ IP アドレスの組（全てのマルチキャストグループを指定する場合には、受信者ホストの IP アドレスのみ）が一つのユーザネームとして登録されており、例えばこの実施例では、IGMP Proxy として機能する CE ルータ 2 2, 2 3 を用いているので、ユーザネームは、CE ルータの IP アドレス、例えば CE ルータ 2 2 の IP アドレス“201.1.1.1”とグループ IP アドレス“224.1.1.1”を組み合わせた“201.1.1.1-224.1.1.1”とし、パスワードは、“RADIUS-CLIENT”としている。

#### 【 0 1 3 0 】

なお、このパスワードは、ユーザ PC に個別に設定されるものではなく、RADIUS のパケットの中で使われるパスワードで、RADIUS のプロトコル上、RADIUS のクライアントを認証するために予め決められたものを登録しておく。

#### 【 0 1 3 1 】

また、“Multicast-Time-Start”の値としては、例えば“Apr 6 21:00:00 JST 2001”、すなわち日本標準時間2001年4月6日の21時00分00秒の開始とし、“Multicast-Time-End”の値としては、例えば“Apr 6 22:00:00 JST 2001”、すなわち日本標準時間2001年4月6日の22時00分00秒の終了を登録しておく。

## 【0132】

また、配信受付サーバ33は、図15に示すように、PEルータ30とポートを介して接続され、Web上で伝送される配信申し込みのためのwwwのパケットを取り込むLANインタフェース33aと、LANインタフェース33aで取り込まれたパケットを受信するパケット受信部33bと、受信されたwwwのパケットのユーザ情報に基づいてユーザを認証するwwwサーバ処理部33cと、配信受付を行う配信受付制御部（WEBサーバ）33dと、ユーザのアカウント名、ユーザのパスワードなどが格納されるユーザデータベース33eと、ユーザ情報をユーザ認証サーバ32に出力するユーザ認証サーバインタフェース（CGI：Common Gateway Interface）33fと、Web上に配信申し込みのためのwwwのパケットを送信するパケット送信部33gとから構成されている。

## 【0133】

この配信受付制御部33dは、受信されたパケットのユーザ情報をCGIなどを用いてデータベースへ展開し、この展開したデータを出力する認証サーバインタフェース33fを介してユーザ認証サーバ32に送信している。

## 【0134】

ユーザデータベース33eは、図16に示すように、ユーザのアカウント名と、ユーザのパスワードの他に、ユーザの接続されているPEルータのポートのIPアドレスと、そのポートのポート番号が格納されている。

## 【0135】

課金サーバ34は、たとえば定額制または従量制によって課金することができる、ここで定額制の課金の場合には、たとえば月単位に定額とし、この定額で参加できるコンテンツは、いつ申し込んでも配信を受けることができるように設定

する。

【0136】

また、従量制の課金の場合には、ユーザ認証サーバ32による認証後に、実際にマルチキャストストリームが流れる時点で、PEルータがストリーム配信を検出し、課金サーバ34にデータを送信する。課金サーバ34は、接続時間を記録し、コンテンツ、接続時間に応じて課金を行う。

【0137】

このような構成のマルチキャスト認証システムにおける配信申し込みからユーザ認証およびコンテンツのストリーム配信に至る一連の動作を図17から図23のフローチャートに基づいて説明する。

【0138】

図17は、PEルータ30による受信パケットの識別動作を示すフローチャートである。図において、図11に示したLANインターフェース30aにあるパケットが取り込まれ、そのパケットがパケット受信部30bで受信されると（ステップ101）、パケット受信部30bでは、受信したパケットがIGMPメンバーシップ・レポートのメッセージパケットかどうか判断する（ステップ102）。

【0139】

なお、この受信パケットの識別は、例えば図4、図5に示したIGMPメンバーシップ・レポートのメッセージの場合で説明すると、まずパケット受信部30bは、MACヘッダの宛先アドレスが自ルータ30宛かどうか判断し、自ルータ30宛ならMACのタイプがIPかどうか判断し、IPならIPヘッダを検索してIPヘッダの宛先アドレスが自ルータ30宛かどうか判断し、自ルータ30宛ならIPのタイプがIGMPかどうか判断し、IGMPならIGMPのタイプが0x16ならIGMPのメンバーシップ・レポートのメッセージであると識別する。

【0140】

ここで、上記受信パケットがIGMPメンバーシップ・レポートのメッセージパケットの場合には、上記受信パケットをIGMP制御部30cに出力し、IG



MP制御部30cによる処理に移行し(ステップ103)、また上記受信パケットがIGMPメンバーシップ・レポートのメッセージでない場合には、RADIUSメッセージパケットかどうか判断する(ステップ104)。

#### 【0141】

ここでも同様に各ヘッダ内の宛先アドレスとタイプを検索し、RADIUSメッセージパケットの場合には、上記受信パケットを認証制御部30dに出力し、認証制御部30dによる処理に移行し(ステップ105)、また上記受信パケットがRADIUSメッセージパケットでない場合には、マルチキャストパケットかどうか判断する(ステップ106)。

#### 【0142】

ここでもMACヘッダの宛先アドレスを検索し、宛先がCEルータの場合には、マルチキャストパケットと判断し、上記受信パケットをマルチキャストフォワーディング制御部30eに出力し、マルチキャストフォワーディング制御部30eによる処理に移行し(ステップ107)、また上記受信パケットがマルチキャストパケットでない場合には、上記受信パケットをパケット受信部30b内で受信処理を行い(ステップ108)、例えばこの受信パケットをパケット送信部30hから送信する。このような工程を行うものには、例えばユーザPC20、21とストリームコンテンツ配信サーバ31間で送受信される参加申し込み用のパケットなどが考えられる。

#### 【0143】

次に、配信受付サーバ33の配信受付の動作について、図18のフローチャートを用いて説明する。

#### 【0144】

この配信受付を動作を説明する前に、まず、サービス事業者は、IP網29を介して配信するコンテンツの予定表をWebページで公開しており、ユーザは、このWebページを閲覧し、ユーザ登録を行い、ユーザのアカウント名とパスワードの発行を受ける。例えば、受信者ホスト20の場合には、アカウントとパスワードは図16に示した“Tokyo”と“t2skf21er4”、また受信者ホスト21の場合には、同様に“Oosaka”と“udfj49t8f”の発行を受ける。

## 【0145】

ユーザ事業者は、ネットワークのユーザに対して、マルチキャストコンテンツ配信用のアカウントを作成している。ユーザ登録を行ったユーザは、例えばユーザPC20のブラウザを立ち上げ、サービス事業者が公開するコンテンツ予定表を提示しているwwwサーバへ接続し、配信の申し込みのためのデータを送る。

## 【0146】

このデータは、wwwのパケットからなり、CEルータ22で中継処理された後、PEルータ30で上述したパケットの識別がなされて配信受付サーバ33に送信される。

## 【0147】

配信受付サーバ33は、図18に示すように、LANインタフェース33aで取り込まれた上記パケットをパケット受信部33bで受信している（ステップ201）。

## 【0148】

ここで、受信パケットがwwwのパケットかどうか判断し（ステップ202）、このwwwのパケットでない場合には、不要なパケットとしてこの受信パケットを廃棄する（ステップ203）。また、この受信パケットがwwwのパケットの場合には、パケット受信部33bは、この受信パケットをwwwサーバ処理部33cに出力し、ユーザのアカウントとパスワードが配信受付制御部33dに出力され（ステップ204）、ここで、配信受付のための処理、例えばユーザのアカウント名とパスワードをデータベース33eでチェックし、ユーザの認証を行う（ステップ205）。

## 【0149】

ここで、ユーザに対して認証がなされないと、例えば正しい設定がなされていないと判断して、配信申し込みの受け付けを拒否し（ステップ206）、またユーザ認証がなされると、PEルータIPアドレスとポート番号と、ユーザのIPアドレスを抽出し、これらのユーザ認証情報を認証サーバインタフェース33fを介してユーザ認証サーバ32のマルチキャスト受信者認証テーブル32eに提供する（ステップ207）。

## 【0150】

このようなパケットの伝送において、ユーザPCとPEルータ30間のCEルータ22は、図19に示すフローチャートに基づいて中継動作を行う。図において、LANインタフェース22aにパケットが取り込まれ、パケット受信部22bで受信されると（ステップ301）、パケット受信部22bでは、受信したパケットがIGMPメンバーシップ・レポートのメッセージパケットかどうか判断する（ステップ302）。

## 【0151】

ここで、この受信パケットがIGMPメンバーシップ・レポートのメッセージパケットでない場合には、通常のデータ通信用のパケットと判断して、この受信パケットをパケット中継処理部22dに出力して通常のパケット中継処理を行う（ステップ303）。また、この受信パケットの場合には、この受信パケットをIGMP Proxy処理部に出力して（ステップ304）、ここでIGMPメンバーシップ・レポートのメッセージパケットの送信元アドレスをユーザPC20のIPアドレスからCEルータ22のIPアドレスに書き換える（ステップ305）。ステップ303または305の処理の後に、パケット送信部22eは、LANインタフェース22aを介してこのパケットを送信する（ステップ306）。

## 【0152】

次に、IGMPメンバーシップ・レポートのメッセージパケットの送受信に伴うPEルータ30とユーザ認証サーバ32の処理動作を図20および図21のフローチャートに基づいて説明する。まず、ユーザPC20から受信したいマルチキャストグループのグループアドレスをIGMPメンバーシップ・レポートのメッセージでPEルータ30に送信すると、PEルータ30は、図17のステップ102においてこのメッセージを認識すると、IGMP制御部30e（図11参照）において、図20の処理フローを実行する。

## 【0153】

図20において、IGMP制御部30cは、受信したIGMPメンバーシップ・レポートのメッセージの送信元IPアドレスとグループIPアドレスを抽出し

(ステップ401)、これらアドレスに基づいてマルチキャスト受信者管理テーブル30fを検索し、エントリの状態に応じて処理を実施する(ステップ402)。

#### 【0154】

次に、ステップ403においてエントリがない場合には、認証制御部30dへの認証処理に移行し(ステップ404)、この送信元IPアドレスと参加要求しているマルチキャストグループのグループIPアドレスによる認証を問い合わせる「Access-Request」のRADIUSメッセージの packets をユーザ認証サーバ32に送信して問い合わせを行う(ステップ405)。

#### 【0155】

この問い合わせの結果、エントリが見つかり、ステップ403では、エントリありと判断されるので、次に現在の状態がユーザ認証サーバによる認証待ちの状態かどうか判断する(ステップ406)。

#### 【0156】

ここで、上記の問い合わせに対して、まだ認証結果を受信していない場合には、認証結果を受信されるまで認証待ちの状態を継続し(ステップ407)、また今の状態が認証待ち状態でない場合には、既に認証済み状態であるかどうか判断する(ステップ408)。

#### 【0157】

ここで、認証済みの状態の場合には、パケット受信部30bは、通常のIGMPの受信処理を行い(ステップ409)、また認証済み状態でない場合には、認証の失敗状態と判断して、IGMPを廃棄する(ステップ410)。このように、認証の失敗状態になると、後述する認証制御部30dの処理動作でマルチキャスト受信者管理テーブル30fの該当エントリが削除されることとなるので、上記動作を繰り返すことがなくなり、ユーザ認証サーバ32への問い合わせが行われる。

#### 【0158】

また、図20のステップ405のように、問い合わせがあると、ユーザ認証サーバ32は、図21のフローチャートに示すように、LANインタフェース32

aで取り込まれ、パケット受信部32bでパケットが受信されると（ステップ501）、パケット受信部32bは、上記受信パケットが問い合わせを示すRADIUSメッセージかどうか判断する（ステップ502）。

## 【0159】

ここで、この受信パケットがRADIUSメッセージでない場合には、受信パケットの廃棄を行う（ステップ503）。また、受信パケットが問い合わせを示すRADIUSメッセージの場合には、認証制御部32cによる認証処理が行われ、RADIUSメッセージ中の受信者のIPアドレスとグループIPアドレスとからなるユーザネームに基づく受信者の認証が行われる（ステップ504）。

## 【0160】

そして、ステップ505において、認証が許可されると、拡張属性であるコンテンツの配信サービスの開始と終了の時間をマルチキャスト受信者認証テーブル32eから読み出し、「Access-Accept」のRADIUSメッセージを作成し（ステップ506）、また認証が不許可の場合には、「Access-Reject」のRADIUSメッセージを作成する（ステップ507）。そして、作成したRADIUSメッセージをパケット送信部32fからLANインタフェース32aを介して送信する（ステップ508）。

## 【0161】

次に、図11に示したPEルータ30の認証制御部30dにおける認証制御の動作について、図22のフローチャートを用いて説明する。図17において、パケット受信部30bがRADIUSメッセージを識別すると、認証制御部30dによる処理に移行し、認証制御部30dは、受信したRADIUSメッセージの内容を確認する（ステップ601）。そして、ユーザ認証サーバ32からの応答が認証の許可かどうか判断する（ステップ602）。

## 【0162】

ここで、この認証が不許可の場合には認証失敗と判断し、マルチキャスト受信者管理テーブル30fから該当するエントリを削除する（ステップ603）。また、この認証が許可された場合には、拡張属性値の時刻を読み出し（ステップ604）、時刻属性があるかどうか判断する（ステップ605）。

## 【0163】

ここで、時刻属性が設定されていない場合には、ユーザ情報をマルチキャスト受信者管理テーブル30fに登録し（ステップ606）、また時刻属性が設定されている場合には、次に現時刻がその拡張属性値の設定時刻内かどうか判断する（ステップ607）。

## 【0164】

ここで、現時刻が設定時刻外、特に設定時刻のスタート時刻前の場合は、例えば内部に有するタイマを起動させて、スタート時刻まで待ち、タイマが満了すると、ユーザ情報をマルチキャスト受信者管理テーブル30fに登録する（ステップ608）。また、現時刻が設定時刻内の場合には、ユーザ情報をマルチキャスト受信者管理テーブル30fに登録する（ステップ606）。

## 【0165】

次に、図11に示したPEルータ30のマルチキャストフォワーディング制御部30eのフォワーディング処理の動作について、図23のフローチャートを用いて説明する。図17において、パケット受信部30bがマルチキャストパケットを識別すると、マルチキャストフォワーディング制御部30eによる処理に移行し、この制御部30eは、受信マルチキャストパケットの宛先アドレス（グループアドレス）をマルチキャストフォワーディングテーブル30gで検索する（ステップ701）。

## 【0166】

そして、このグループアドレスのマルチキャストグループに参加している受信者がいるかどうか判断する（ステップ702）。

## 【0167】

ここで、参加している受信者がいない場合には、このパケットを廃棄し（ステップ703）、受信者がいる場合には、当該受信者がいる受信者ポート番号のポートにパケットをフォワードする（ステップ704）。そして、パケット送信部30hからLANインターフェース30aを介して送信する（ステップ705）。

## 【0168】

このように、この実施例では、参加申し込みにより、予めマルチキャストグループに参加できるユーザPCをユーザ認証サーバに登録しておき、IGMPを用いて、ユーザPCから参加要求を示すメンバーシップ・レポートが送信されると、このレポート内の情報とこのユーザ認証サーバの登録内容に基づいてユーザPCの認証がなされ、認証されると許可時間内のマルチキャストグループへの当該ユーザPCの参加を許可することにより、ユーザPCの機能は既存の仕組みのままで、ユーザPCを正確に認証することができる。

## 【0169】

また、この実施例では、マルチキャストグループへ参加できる許可時間がユーザ認証サーバに設定されているので、認証によって参加を許可されたユーザPCは許可された時間内で、必要な時間だけマルチキャストパケットをフォワードすることができる。

## 【0170】

また、この実施例では、送信元アドレスとグループアドレスの組を一つのユーザネームとして認証を行うので、各ユーザPCに個別のパスワードを設ける必要がなくなり、参加申し込み時や参加要求時の手続きの際に、予め決められているパスワードを入力してユーザ認証サーバに問い合わせることができる。

## 【0171】

なお、この実施例では、ユーザ認証サーバが参加を許可するユーザPCの認証判断を行ったが、この発明はこれに限らず、たとえばPEルータがこの認証の機能を有し、ユーザに対する認証判断を行うことも可能である。この場合には、ユーザ認証サーバはマルチキャスト受信者認証テーブルを有し、PEルータからの要求によってこのテーブルの登録内容をPEルータに送信するように設定する。

## 【0172】

## (実施例2)

実施例1では、PEルータ30がIGMP制御、認証制御およびマルチキャストフォワーディング制御を行う場合について説明したが、この発明はこれに限らず、たとえばCEルータ22、23がこれら制御を行うことも可能である。

## 【0173】

この場合のＣＥルータ２２，２３の構成としては図１１に示したＰＥルータ３０の構成と同じ構成であり、ＰＥルータ３０はパケットの中継機能を有するものとする。

## 【０１７４】

この場合に、例えばユーザの認証をＣＥルータ２２，２３で行うとすると、認証に利用されるＩＧＭＰメッセージのＩＰアドレスが、受信者ＩＰアドレスであるため、各ユーザＰＣ２０，２１のＩＰアドレスがそのまま使用される。

## 【０１７５】

このため、ＣＥルータ２２，２３が有することとなるマルチキャスト受信者管理テーブルは、図１２に示すように、受信者ＩＰアドレスが各ユーザＰＣ２０，２１のアドレス、例えば“１９２．５２．１５０．１”と“１９２．５２．１２２．１”とが格納されており、受信者ポート番号にはこのユーザＰＣのアドレスが格納される。

## 【０１７６】

これにより、この実施例では、参加申し込みにより、予めマルチキャストグループに参加できる受信者ホストをユーザ認証サーバに登録しておき、ＩＧＭＰを用いて、受信者ホストから参加要求を示すメンバーシップ・レポートが送信されると、このレポート内の情報とこのユーザ認証サーバの登録内容に基づいて受信者ホストの認証がなされ、認証されると許可時間内のマルチキャストグループへの当該受信者ホストの参加を許可することにより、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証する。

## 【０１７７】

## (実施例３)

また、この発明にかかる認証システムは、たとえば図２４に示すように、ＦＴＴＨ（Fiber To The Home）サービスの常時接続用のネットワークシステムに用いることも可能である。図において、中央局８０には、ＬＡＮスイッチ８１とコンテンツ・サーバ８２とが存在し、集線局８５にはＬＡＮスイッチ８６が存在し、ユーザ宅９０にはメディア・コンバータ９１と受信者ホスト９２が存在している。

## 【０１７８】

このような構成でも、実施例１と同様に、ＬＡＮスイッチ８１または８６にＩＧ



MP制御、認証制御およびマルチキャストフォワーディング制御の機能を持たせて、コンテンツ・サーバ82の配信サービスを提供できる。また、ユーザの認証を行う手段は、中央局80内に設けても良いし、インターネットの網内に設けても良い。

## 【0179】

これにより、この実施例でも、実施例1と同様に、参加申し込みにより、予めマルチキャストグループに参加できる受信者ホストをユーザ認証サーバに登録しておき、IGMPを用いて、受信者ホストから参加要求を示すメンバーシップ・レポートが送信されると、このレポート内の情報とこのユーザ認証サーバの登録内容に基づいて受信者ホストの認証がなされ、認証されると許可時間内でのマルチキャストグループへの当該受信者ホストの参加を許可することにより、PCの機能は既存の仕組みのままで、ユーザPCを正確に認証することができる。

## 【0180】

この発明は、これら実施形態に限定されるものではなく、この発明の要旨を逸脱しない範囲で種々の変形実施が可能である。たとえばVOD（ビデオ・オン・デマンド）などのビデオ番組のような動画配信サービスにも用いることが可能である。

## 【0181】

## 【発明の効果】

以上説明したように、この発明では、マルチキャストグループに参加できる受信者ホストまたは中継ルータのアドレスを認証サーバに登録しておき、受信者ホストから参加要求を示すIGMPのメンバーシップ・レポートが送信されると、このレポート内の情報とこの認証サーバの登録内容に基づいて受信者ホストの認証がなされ、認証されるとマルチキャストグループへの当該受信者ホストの参加を許可するので、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証することができる。

## 【0182】

また、この発明では、受信者ホストまたは中継ルータのアドレスとともに、当該受信者ホストまたは中継ルータが接続されているルータのポートの情報を認証

サーバに登録しておき、受信者ホストから参加要求を示す I G M P のメンバーシップ・レポートが送信されると、このレポート内の情報とこの認証サーバの登録内容に基づいて受信者ホストの認証がなされ、認証されるとマルチキャストグループへの当該受信者ホストの参加を許可するので、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証することができる。

## 【 0 1 8 3 】

また、この発明では、上記発明において、マルチキャストグループのグループアドレスをさらに認証サーバに登録しておき、受信者ホストから参加要求を示す I G M P のメンバーシップ・レポートが送信されると、このレポート内の情報とこの認証サーバの登録内容に基づいて受信者ホストの認証がなされ、認証されるとマルチキャストグループへの当該受信者ホストの参加を許可するので、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証することができる。

## 【 0 1 8 4 】

また、この発明では、上記発明において、全てのマルチキャストグループへの参加に応じて、受信者ホストまたは中継ルータのアドレスを認証サーバに登録しておき、受信者ホストから参加要求を示す I G M P のメンバーシップ・レポートが送信されると、このレポート内の情報とこの認証サーバの登録内容に基づいて受信者ホストの認証がなされ、認証されるとマルチキャストグループへの当該受信者ホストの参加を許可するので、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証することができる。

## 【 0 1 8 5 】

また、この発明では、上記発明において、マルチキャストグループへの参加を許可する許可時間も認証サーバに登録しておき、受信者ホストから参加要求を示す I G M P のメンバーシップ・レポートが送信されると、このレポート内の情報とこの認証サーバの登録内容に基づいて受信者ホストの認証がなされ、認証されるとマルチキャストグループへの当該受信者ホストの参加を許可するので、受信者ホストの機能は既存の仕組みのままで、受信者ホストを正確に認証することができる。

【0186】

また、この発明では、上記の認証の機能に課金の機能を組み合わせることで、正確に課金できるようになり、これによってサービス事業者が有料でコンテンツを配信することが可能となる。

【図面の簡単な説明】

【図1】

この発明にかかるマルチキャスト認証システムの概略構成を示す構成図である。

【図2】

図1に示したユーザ認証サーバが有するマルチキャスト受信者認証テーブルの構成の一例を示す構成図である。

【図3】

図1に示したシステムの各部の動作を示すタイムチャートである。

【図4】

IGMPのメンバーシップ・レポートメッセージのフォーマットを示す図である。

【図5】

図4に示したIGMP Messageのフォーマットを示す図である。

【図6】

RADIUSメッセージのフォーマットを示す図である。

【図7】

図6に示したRADIUS Messageのフォーマットを示す図である。

【図8】

図7に示したAttributesのフォーマットを示す図である。

【図9】

この発明にかかるマルチキャスト認証システムの実施例1の構成を示す構成図である。

【図10】

図9に示したCEルータの構成の一例を示す構成図である。

【図 1 1】

図 9 に示した P E ルータの構成の一例を示す構成図である。

【図 1 2】

図 1 1 に示したマルチキャスト受信者管理テーブルの構成を示す構成図である。

【図 1 3】

図 1 1 に示したマルチキャストフォワーディングテーブルの構成を示す構成図である。

【図 1 4】

図 9 に示したユーザ認証サーバの構成の一例を示す構成図である。

【図 1 5】

図 9 に示した配信受付サーバの構成の一例を示す構成図である。

【図 1 6】

図 1 5 に示したデータベースの構成の一例を示す構成図である。

【図 1 7】

図 1 1 に示した P E ルータによる受信パケットの識別動作を示すフローチャートである。

【図 1 8】

図 1 5 に示した配信受付サーバの配信動作を説明するためのフローチャートである。

【図 1 9】

図 1 0 に示した C E ルータの中継動作を説明するためのフローチャートである。

【図 2 0】

図 1 1 に示した I G M P 制御部の制御動作を説明するためのフローチャートである。

【図 2 1】

図 1 4 に示したユーザ認証サーバの認証動作を説明するためのフローチャートである。

【図 2 2】

図 1 1 に示した認証制御部の認証動作を説明するためのフローチャートである。

【図 2 3】

図 1 1 に示したマルチキャストフォワーディング制御部のフォワーディング処理の動作を説明するためのフローチャートである。

【図 2 4】

この発明にかかるマルチキャスト認証システムの実施例 3 の構成を示す構成図である。

【図 2 5】

従来のマルチキャスト認証システムの概略構成を示す構成図である。

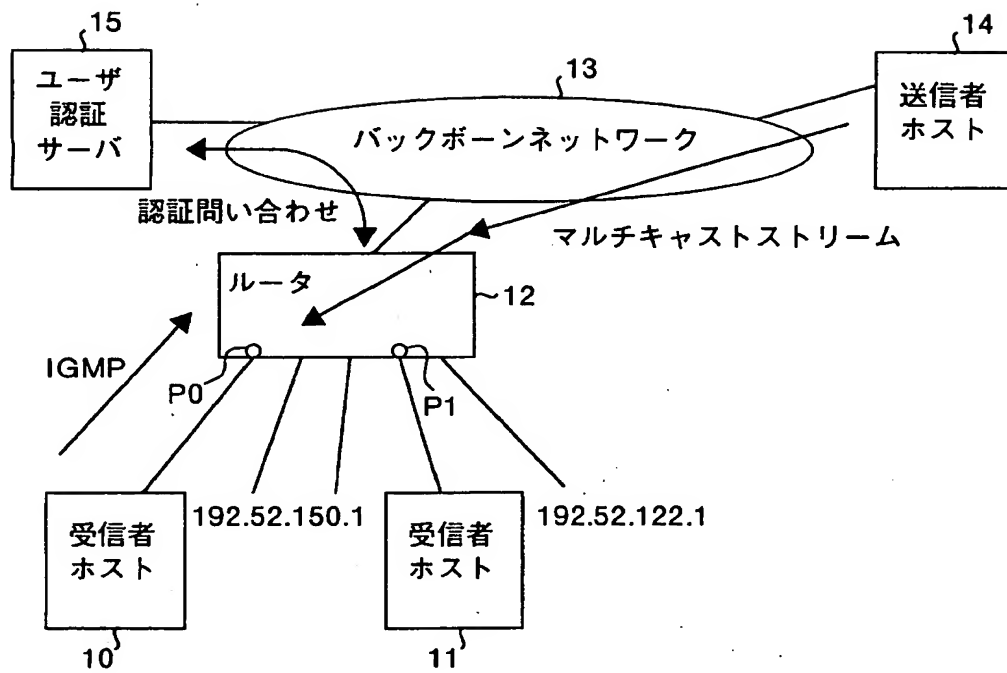
【符号の説明】

- 1 0, 1 1, 2 0, 2 1, 9 2 受信者ホスト (ユーザ P C)
- 1 2 ルータ
- 1 3 バックボーンネットワーク
- 1 4 送信者ホスト
- 1 5 ユーザ認証サーバ
- 2 2, 2 3 C E ルータ
- 2 2 a, 3 0 a, 3 2 a, 3 3 a L A N インタフェース
- 2 2 d パケット中継処理部
- 2 2 c I G M P P r o x y 処理部
- 2 2 b, 3 0 b, 3 2 b, 3 3 b パケット受信部
- 2 2 e, 3 0 h, 3 2 f, 3 3 g パケット送信部
- 2 9 I P 網
- 3 0 P E ルータ
- 3 0 c I G M P 制御部
- 3 0 d 認証制御部
- 3 0 e マルチキャストフォワーディング制御部
- 3 0 f マルチキャスト受信者管理テーブル
- 3 0 g マルチキャストフォワーディングテーブル

- 3 1 ストリームコンテンツ配信サーバ
- 3 2 ユーザ認証サーバ
  - 3 2 c 認証制御部
  - 3 2 d 配信受付サーバインタフェース
  - 3 2 e マルチキャスト受信者認証テーブル
- 3 3 配信受付サーバ
  - 3 3 c w w wサーバ処理部
  - 3 3 d 配信受付制御部
  - 3 3 e ユーザ認証サーバインタフェース
  - 3 3 f 認証サーバインタフェース
- 3 4 課金サーバ
- 8 0 中央局
- 8 1, 8 6 スイッチ
- 8 2 コンテンツ・サーバ
- 8 5 集線局
- 9 0 ユーザ宅
- 9 1 メディア・コンバータ

【書類名】 図面

【図 1】



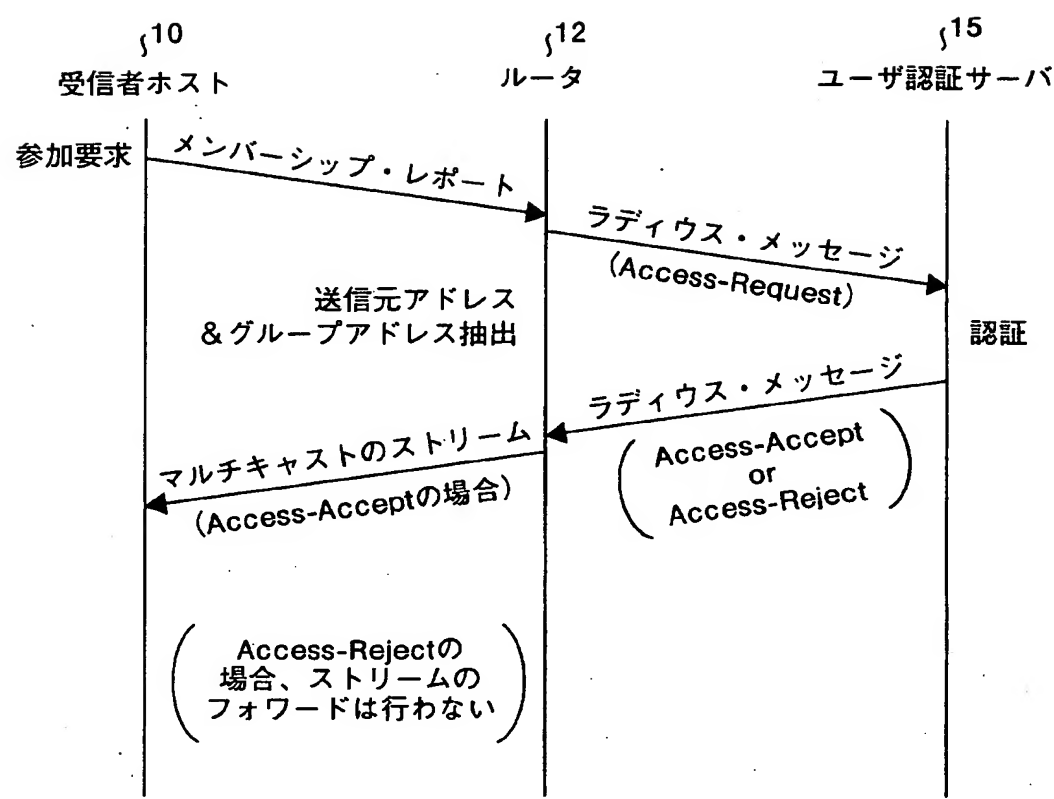
【図 2】

マルチキャスト受信者認証テーブル

受信者IPアドレス	グループアドレス	PEルータIPアドレス	PEルータポート番号
192.52.150.1	224.1.1.1	220.0.0.1	1
192.52.122.1	なし(全部許可)	220.0.0.2	6



【図 3】



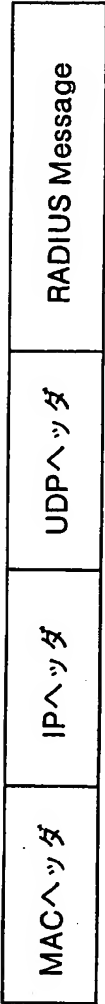
【図 4】



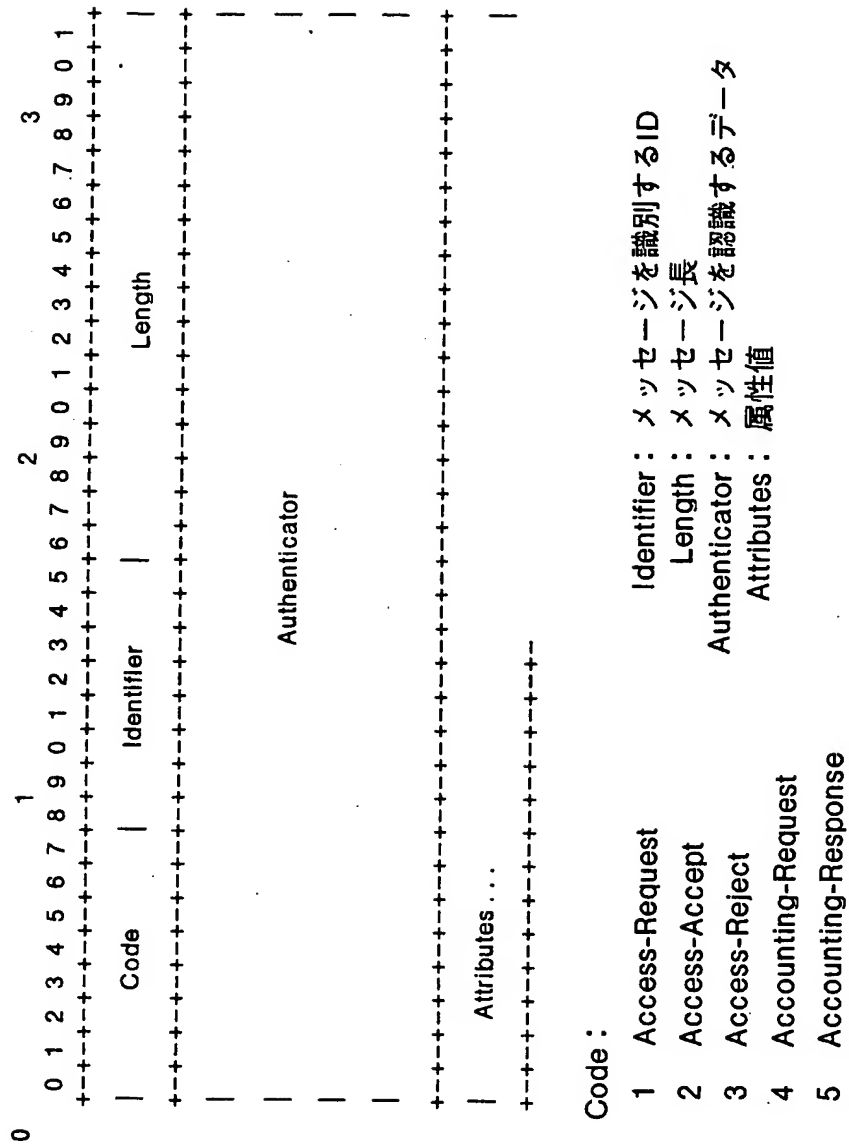
【図 5】

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Type										Max Resp Time										Checksum																			
Group Address																																							

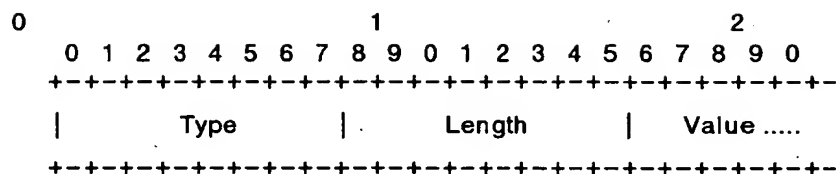
【図 6】



【図 7】



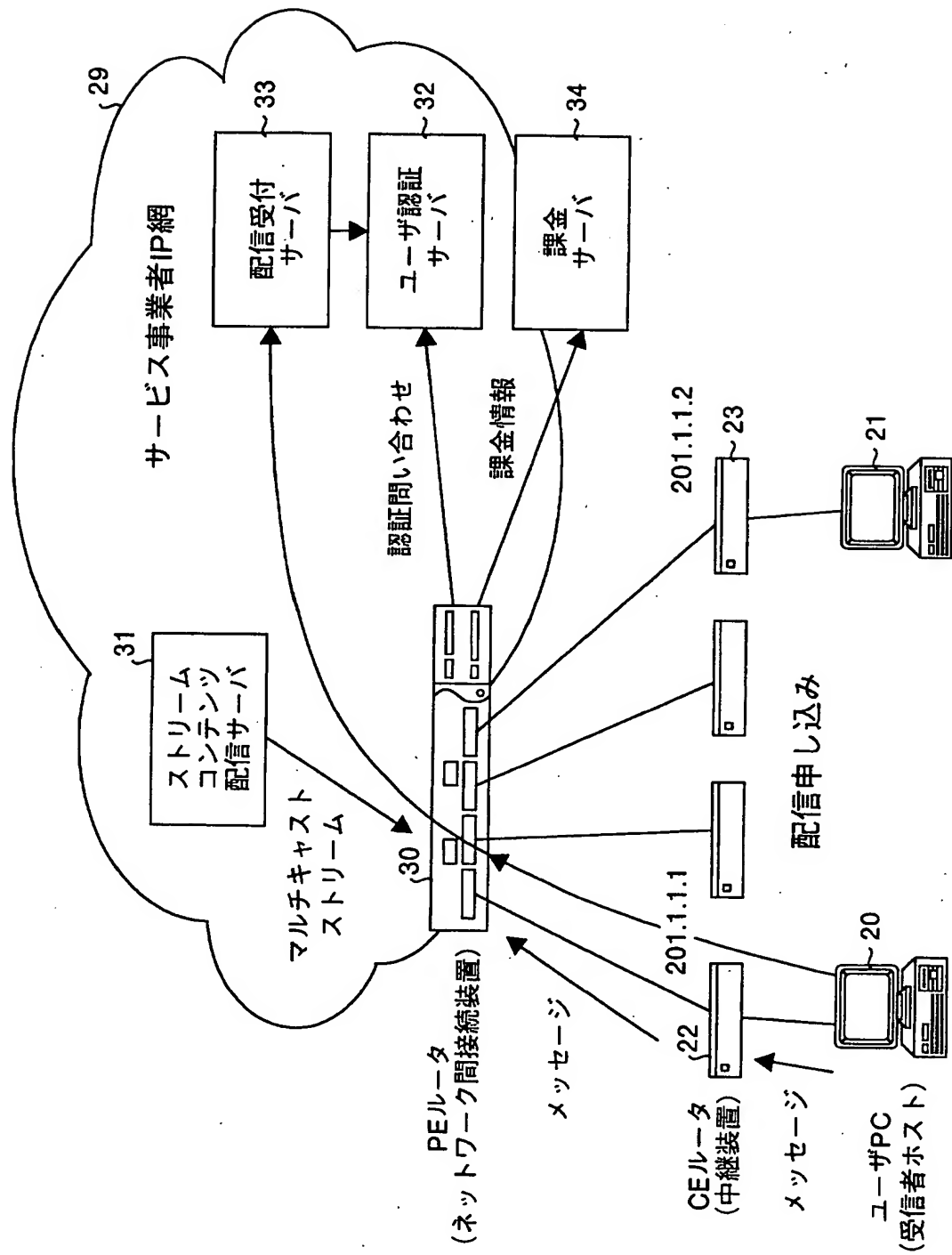
【図 8】



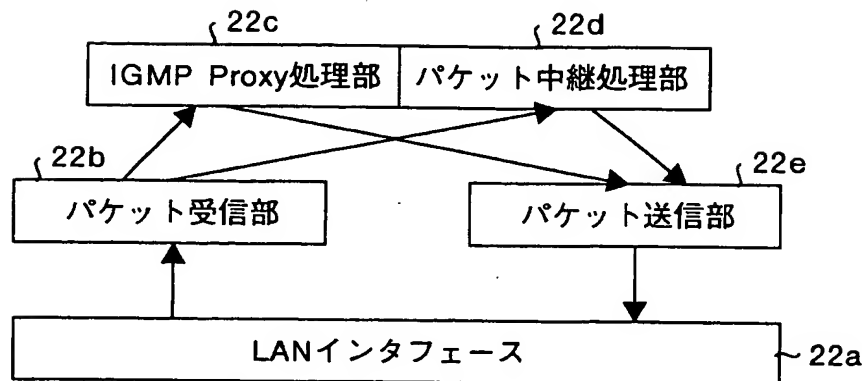
Type

- 1 User-Name
- 2 User-Password
- 4 NAS-IP-Address
- 5 NAS-Port
  
- 223 Multicast-Time-Start
- 224 Multicast-Time-End

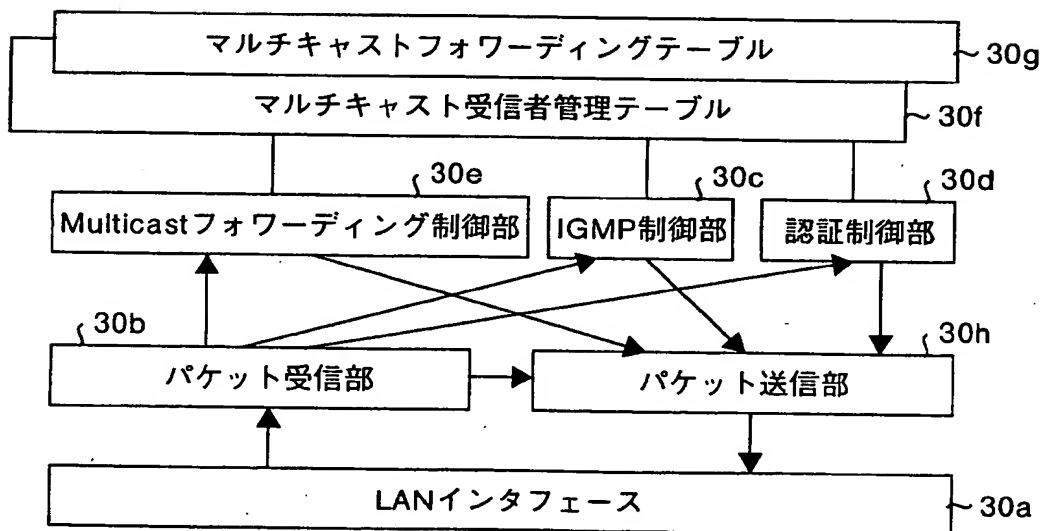
【図9】



【図10】



【図11】



【図 12】

マルチキャスト受信者管理テーブル

グループアドレス	受信者IPアドレス	受信者ポート番号	送信者ポート番号
224.1.1.1	201.1.1.1 (192.52.150.1)	1	15
224.1.1.2	201.1.1.2 (192.52.122.1)	2	16



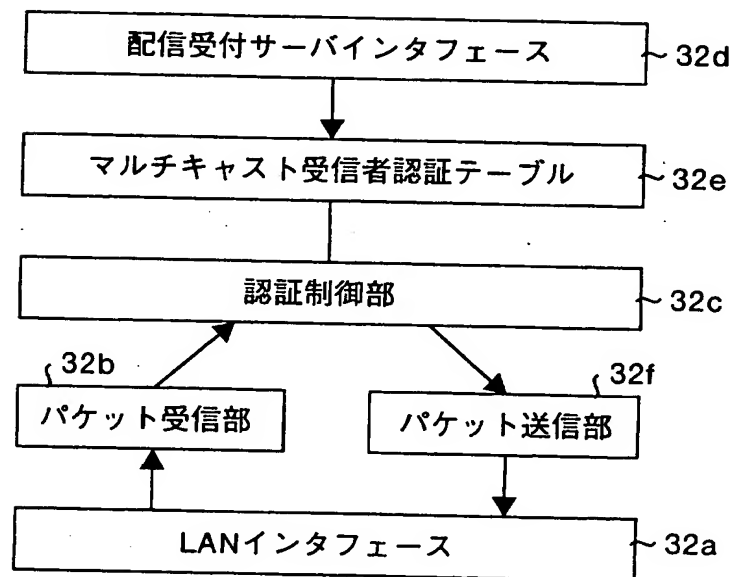
【図 1 3】

マルチキャストフォワーディングテーブル

グループアドレス	受信者ポート番号リスト
224.1.1.1	1,3,4,6, .....
224.1.1.2	2,3,5,8, .....

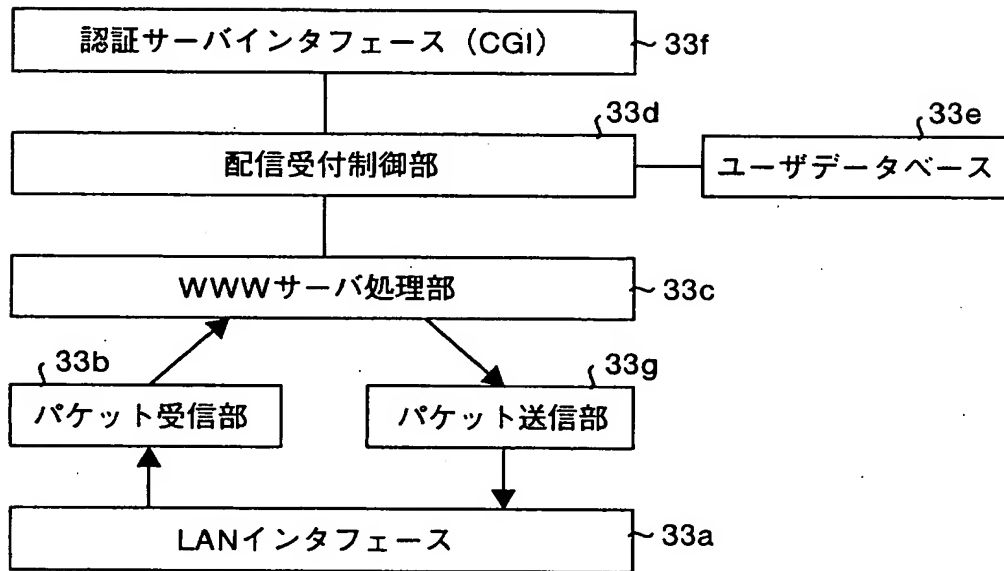
【図 1 4】

ユーザ認証サーバ



【図 1 5】

配信受付サーバ

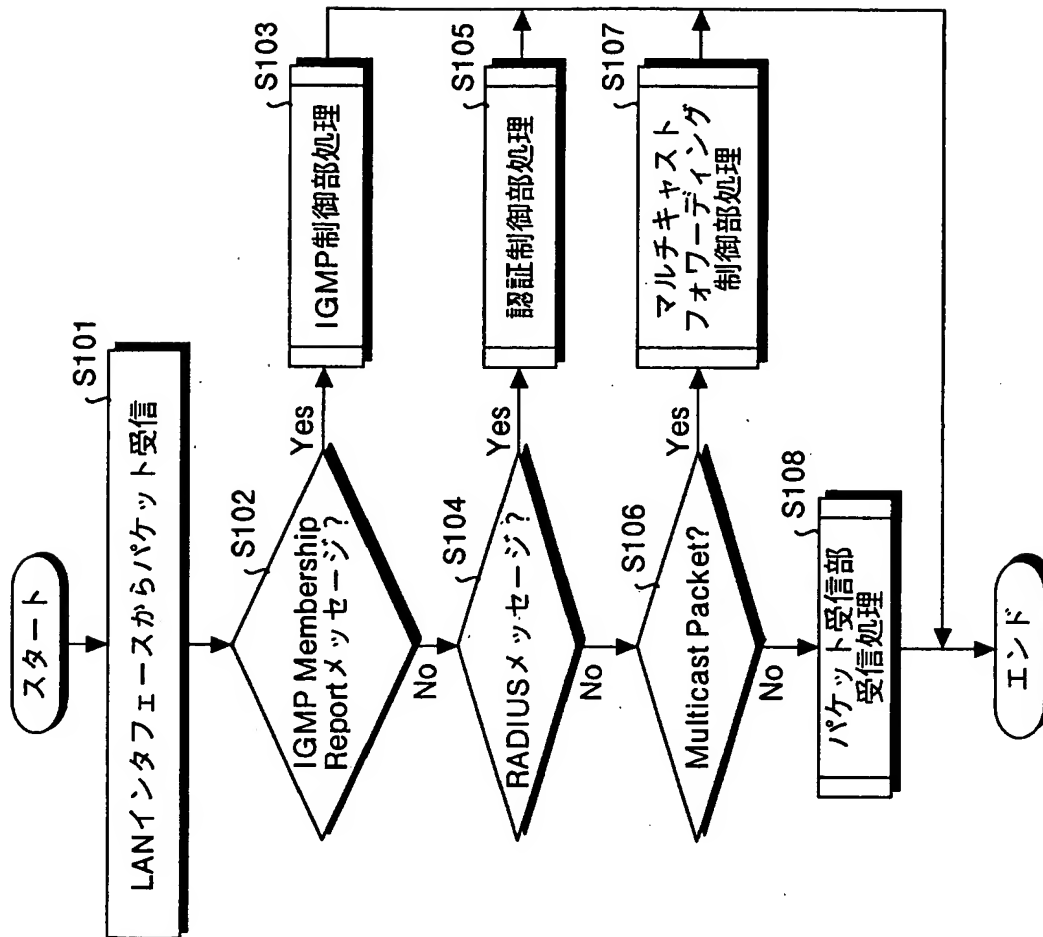


【図 1 6】

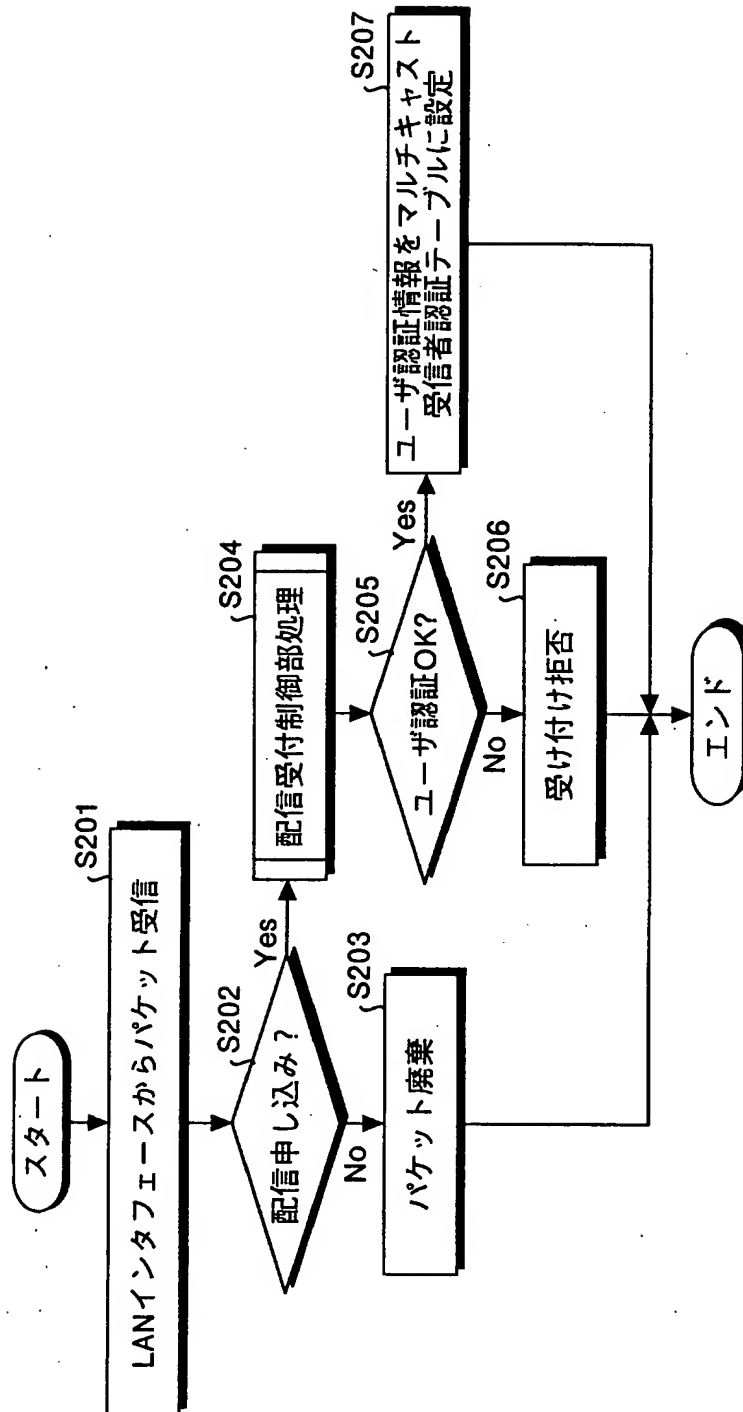
配信受信サーバデータベース

ユーザアカウント名	ユーザハッシュ	受信者IPアドレス	PEL-タイプアドレス	PEL-ポート番号
Tokyo	t2skf21er4	192.52.150.1	220.0.0.1	1
Oosaka	udfj49t8f	192.52.122.1	220.0.0.2	6

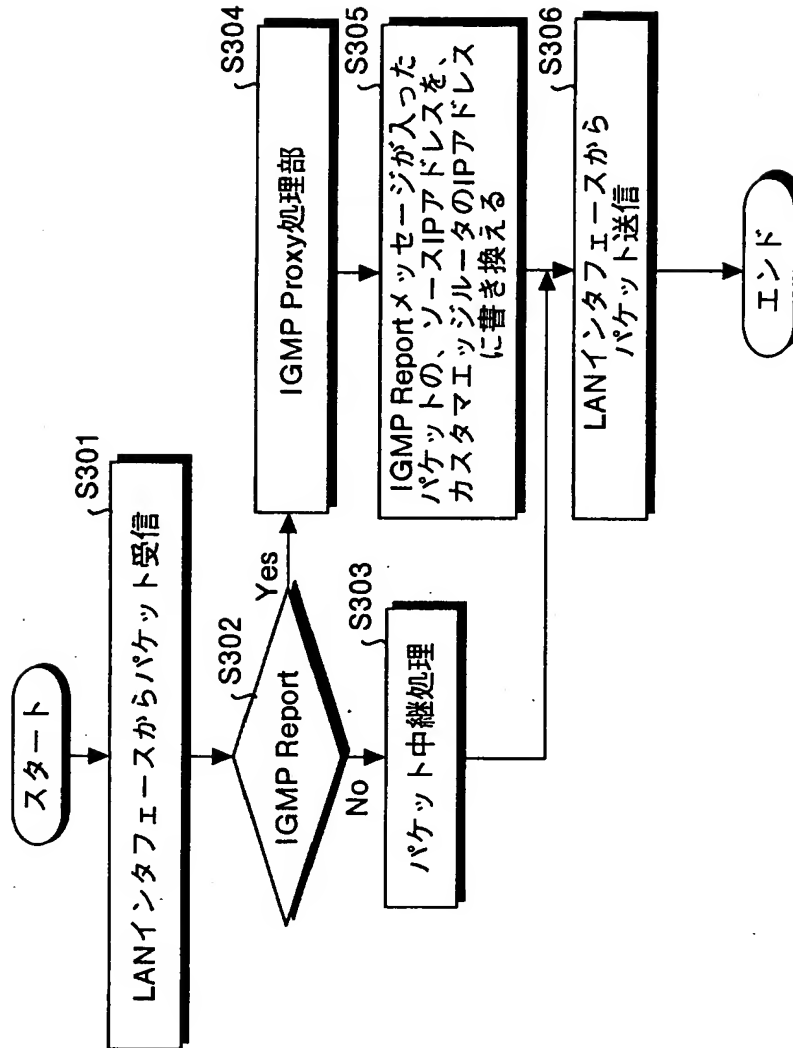
【図 17】



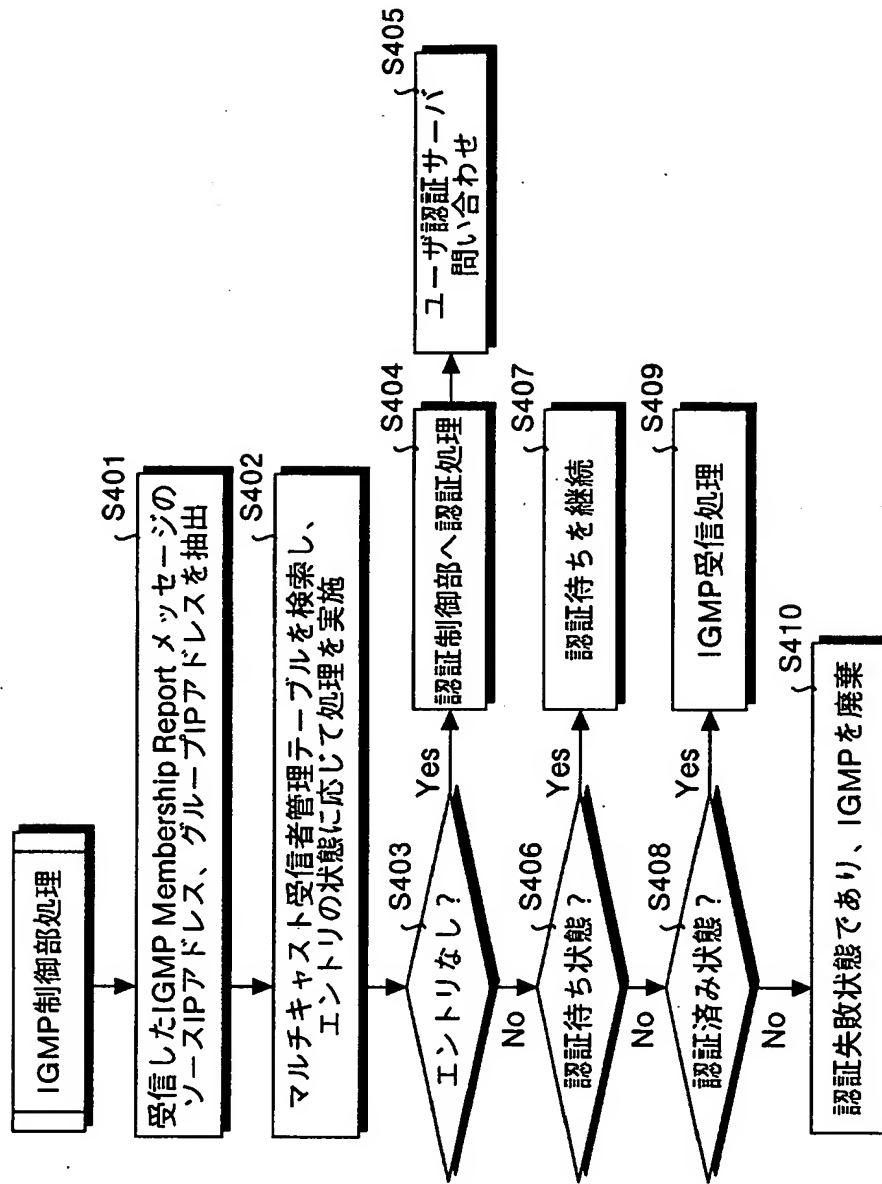
【図 1 8】



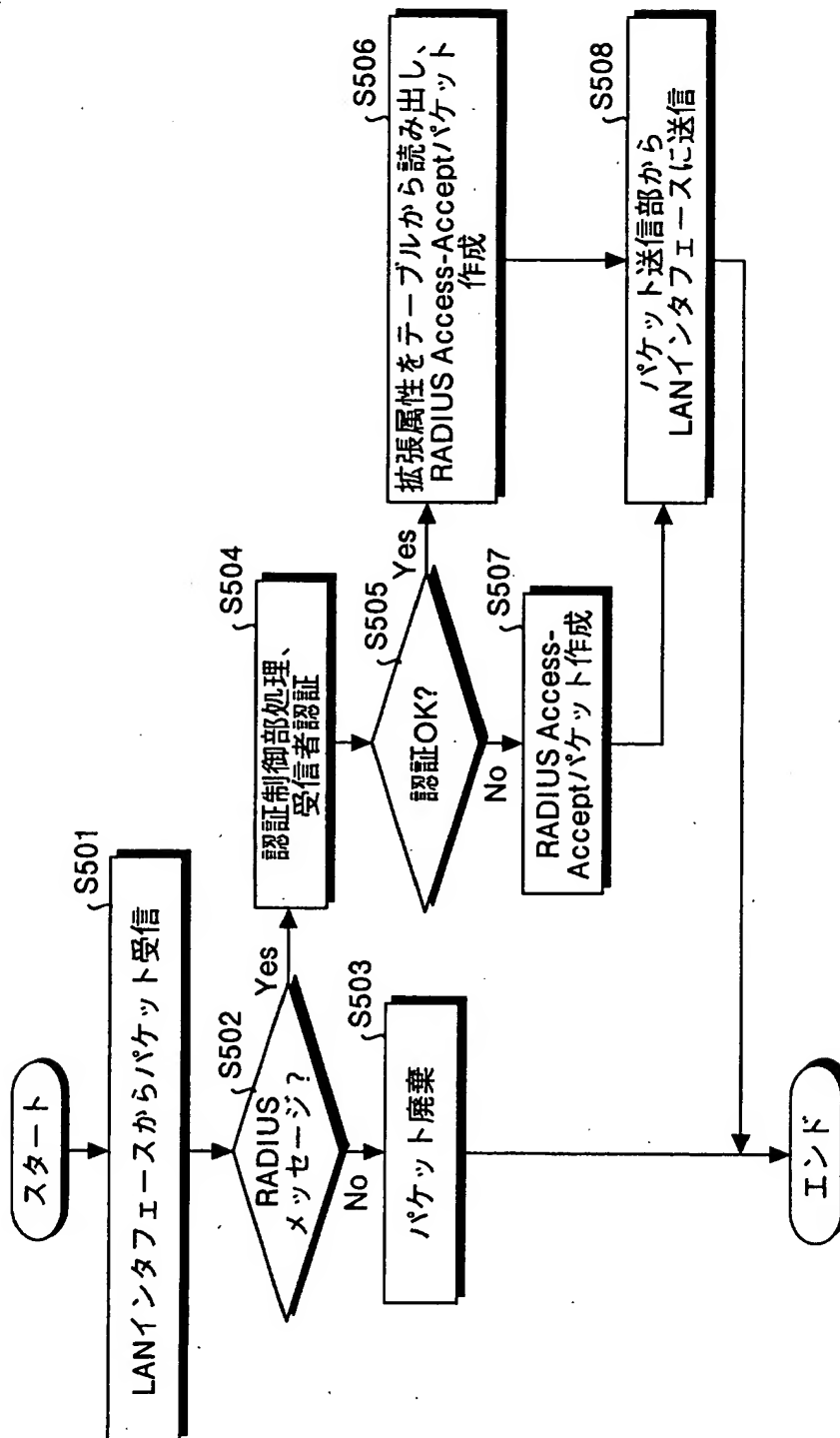
【図19】



【図 2 0】

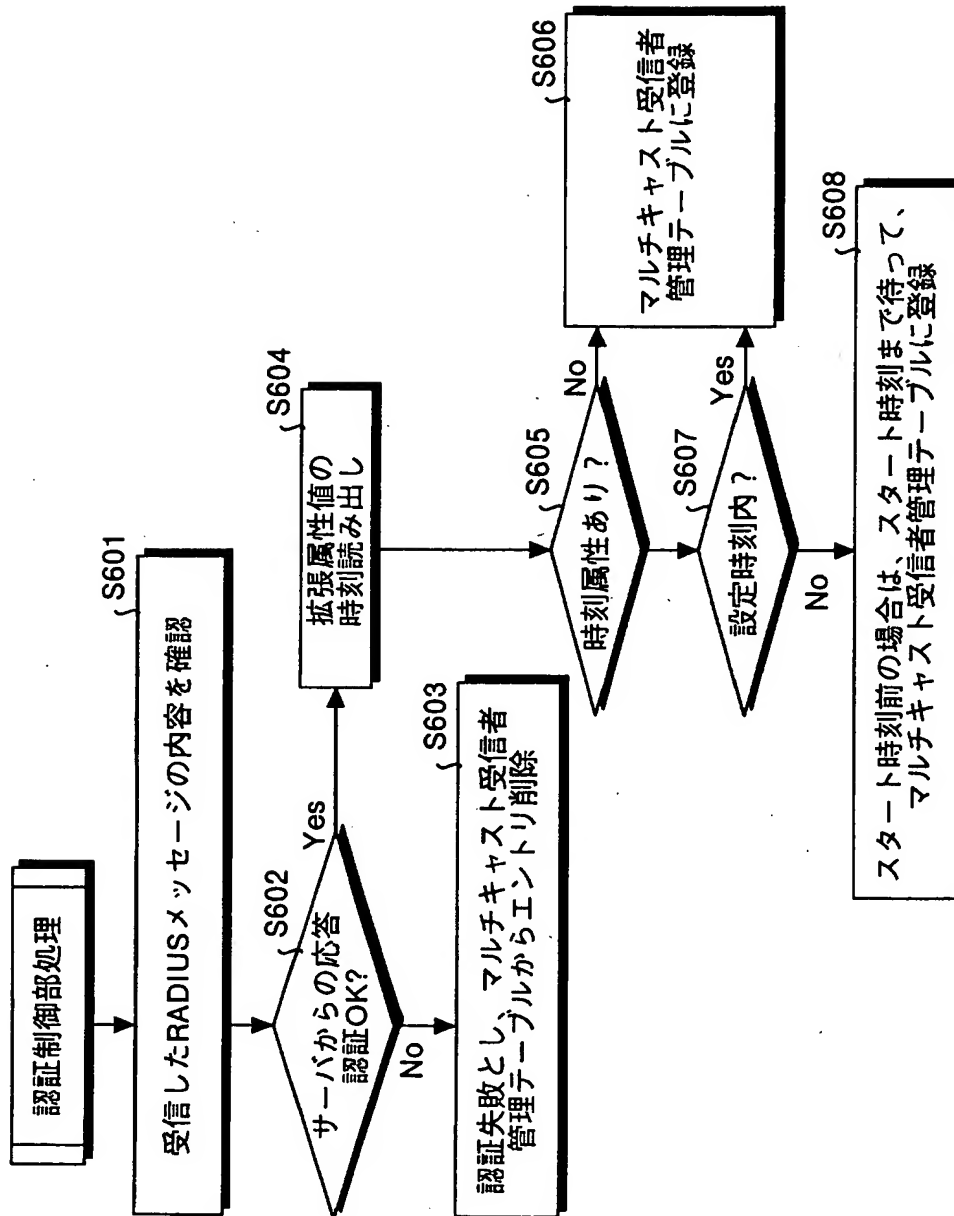


【図 21】

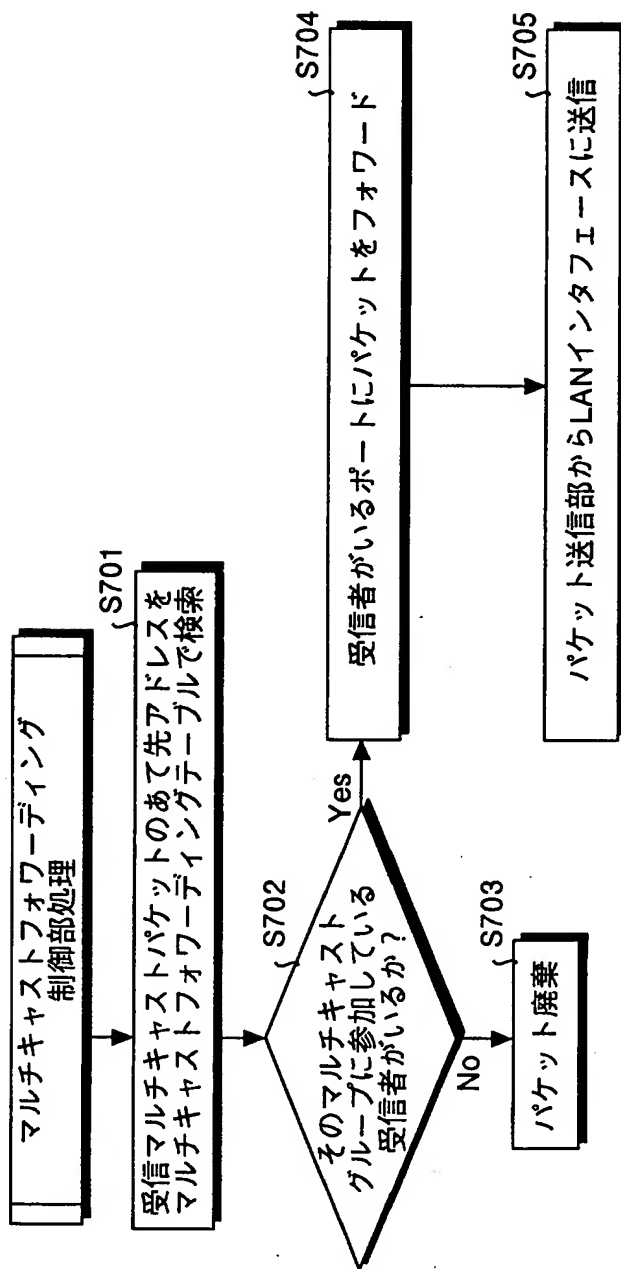




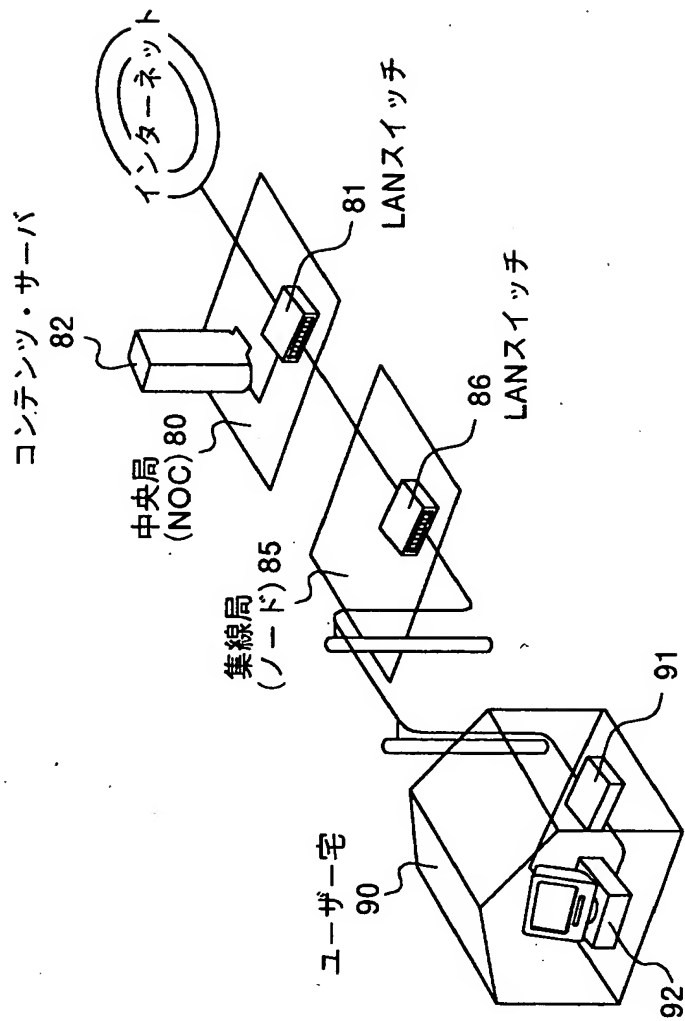
【図 22】



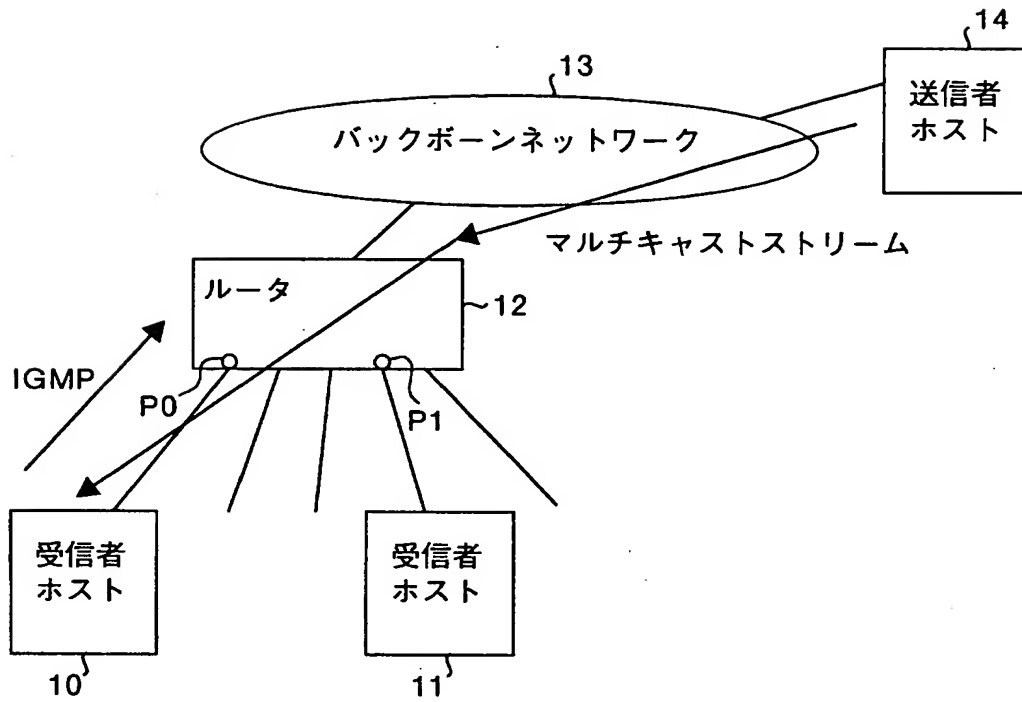
【図 23】



【図 24】



【図 25】



【書類名】 要約書

【要約】

【課題】 受信者側のホストの機能は既存の仕組みのままで、ユーザを正確に認証する。

【解決手段】 受信者ホスト 1 0, 1 1 からの参加申し込みにより、予めマルチキャストグループに参加できる受信者ホスト 1 0, 1 1 をユーザ認証サーバ 1 5 に登録しておき、受信者ホストから参加要求を示す I G M P のメンバーシップ・レポートがルータ 1 2 に送信されると、このレポート内の情報とこのユーザ認証サーバ 1 5 の登録内容に基づいて受信者ホスト 1 0, 1 1 の認証がなされ、認証されると許可時間内でのマルチキャストグループへの受信者ホスト 1 0, 1 1 の参加を許可する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005290]

1. 変更年月日 1990年 8月29日

[変更理由] 新規登録

住 所 東京都千代田区丸の内2丁目6番1号

氏 名 古河電気工業株式会社